INTERNET GOVERNANCE

ICANN Guide for Law Enforcement

Table of Contents

PREAMBLE: Why Is ICANN Important To Public Safety Agencies?

ICANN is the top level coordination body of the Internet. ICANN's role is to oversee the complex interconnected network of unique identifiers, i.e. the Domain Name System (DNS); Internet Protocol (IP) addresses and Autonomous System Numbers (ASN); and protocols and parameters - all of which allow computers on the Internet to communicate.

The Internet is governed by the "multi-stakeholder" model and NOT by international laws, regulations or treaties. ICANN is at the center of the multi-stakeholder model, a unique form of governance that uses a bottom-up decision making process. Therefore, it is a decentralized, inclusive and participatory process that includes all stakeholders (private industry, government, civil society, etc.). Within this system, law enforcement, consumer protection and other public safety agencies are not afforded special status. To be effective, only the most vocal, prepared and persistent are able to affect policy, protocols and standards changes. Therefore, it is critical for public safety agencies to participate in an active and meaningful way at ICANN.

DNS and its Impact on Public Safety:

This booklet is meant as a high-level introduction to ICANN and some, not all, of the issues concerning the DNS and investigations, especially domain name registrations. A few key issues and components of the ICANN-administered DNS are critical:

- Registry Agreement – The contract between ICANN and gTLD registries containing obligations for domain names at the highest level.
- Registrar Accreditation Agreement – The contract between ICANN & gTLD registrars containing obligations for domain name registrations by customers.
- WHOIS – The Internet's digital phonebook, key for attribution of domain names.

Public Safety Agencies at ICANN are dedicated to:

1. Assessing whether and seeking to ensure that the Domain Name System (DNS) and domain name registrations are not used to propagate, enhance, or further, unlawful activity, abuse, consumer fraud, deception, or malfeasance, and/or violations of law;
2. Supporting the ability of public safety organizations to investigate, prevent, attribute, and disrupt unlawful activity, abuse, consumer fraud, deception or malfeasance, and/or violations of national law that involve the DNS and domain name registrations;
3. Cooperating with ICANN's advisory committees (including the RSSAC, SSAC), supporting organizations (including the GNSO, ASO, ccNSO), and community, to ensure multi-stakeholder support and cooperation, in advancing public safety policies, recommendations, and advice;
4. Participating in applicable ICANN working/study groups to promote a shared understanding of the potential effects such groups' work and recommendations will have on public safety;
5. Continuously assessing whether ICANN has responsive and timely mechanisms to develop and enforce ICANN contractual obligations with gTLD registries and registrars, (*i.e.*, Registrar Accreditation Agreement, Registry Agreement); and
6. Addressing work streams, policies, and studies that are brought forth at ICANN that affect public safety.

General ICANN Information

ONE WORLD, ONE INTERNET

WHAT DOES ICANN DO?

To reach any device or thing connected to the Internet, you (or your search engine) must know their address – a name or a number. That address must be unique, so you can reliably find and connect to other devices, things, or information sources no matter where you are in the world. That's how the tens of thousands of physical networks appear and operate as 'One Internet'.

In concert with the technical operating community, ICANN maintains and administers the registries containing these unique addresses across the world ensuring the security, stability, and integrity of One Internet where we can reliably find each other.

Community-Driven Global Policy Development

To keep pace with dynamic technologies and rapid innovation, ICANN facilitates an open, consensus-driven, multistakeholder policy development process that is run from the bottom up.

Multistakeholder Model

Civil Society & Internet Users, the Private Sector, National & International Organizations, Governments, Research, Academic and Technical Communities are all represented.

Competition & Choice

From accrediting over 1000 registrars, to introducing new Top Level Domains (TLDs), ICANN works to expand consumer choice by fostering competition and innovation in the domain name marketplace.

WHICH FUNCTIONS DOES ICANN COORDINATE?

DNS
- Development of generic TLD policy
- Facilitation of country code TLD policy discussions
- Delegation of and changes to Top-level domains
- Management of the root's DNSSEC trust anchor
- Facilitating Root Server System discussions

Internet Numbers
- Approval of global number allocation policies
- Allocation of top-level blocks of Internet numbers
- Recognize Regional Internet Registries

Protocol Parameters
- Creation of and changes to protocol parameter registries
- Management of the Time Zone Database

Security & Stability

ICANN supports DNS security by supporting a secured DNS infrastructure (DNSSEC) and managing the top-level key of that infrastructure, requiring close coordination and collaboration with the community and volunteers around the world.

Interoperability

ICANN's work plays a role in helping the community to develop new technologies that flourish while maintaining interoperability across the global Internet. For example, the central publication point of unique protocol identifiers maintained by ICANN makes it easier for protocol developers to create protocols that allow communications using secure connections between users.

Contractual Compliance

ICANN maintains the contracts and enforces the consensus policies developed through the community-driven process embodied in those contracts. While we are not a regulator, we comply with the law and enforce community policies through contractual obligations.

HOW DO I PARTICIPATE?

- Sign up for updates at icann.org
- Join one of the many Public Comment Forums on ICANN's website
- Attend ICANN's Public Meetings in person or online to provide input at a Public Forum
- Join one of ICANN's Supporting Organizations or Advisory Committee
- Follow us on Twitter, Facebook, LinkedIn
- Subscribe to newsletters
- Participate in our fellows program
- Join a regional engagement group

WHO'S INVOLVED?

A number of groups, each of which represents a different interest and expertise on the Internet.
All of them come together with the Board of Directors to shape policies and ICANN work.

Supporting Organizations
- Addressing
- Country Code Names
- Generic Names

Advisory Committees
- At-Large
- Governmental
- Root Server System
- Security & Stability

Technical Advisory Bodies
- Technical Experts Group
- Technical Liaisons from IETF, ETSI, W3C, ITU

Board of Directors
- 16 Community Appointed Board Members

XPLANATIONS by XPLANE.com

ICANN Board of Directors

Voting Seats

Non-Voting Seats

Ombudsman

Board of Directors

Nominating Committee

+ Per ICANN Bylaws, Article VII, Section 2

ASO

+ Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC)

ccNSO

+ ccTLD registries (.us, .uk, .au, .be, .nl, etc.)

GNSO

+ gTLD registries
+ gTLD registrars
+ IP interests
+ ISPs
+ Businesses
+ Non-commercial interests
+ Not-for-Profit Operational Concerns

At-Large

+ Per ICANN Bylaws: At-large Advisory Committee, in conjunction with RALOs (ALAC)

President and CEO

+ ICANN staff

Internet Engineering Task Force (IETF)

Security and Stability Advisory Committee (SSAC)

Root Server System Advisory Committee (RSSAC)

Governmental Advisory Committee (GAC)

What is ICANN?

ICANN is a not-for-profit, public-benefit organization formed in 1998. Its staff operates the Internet's Domain Name System, coordinates allocation and assignment of the Internet's unique identifiers, such as Internet Protocol addresses, accredits generic top-level domain (gTLD) name registrars, and helps facilitate the voices of volunteers worldwide who are dedicated to keeping the Internet secure, stable and interoperable. ICANN promotes competition in the domain name space and helps develop Internet policy.

How is ICANN organized?

At the heart of ICANN's policy-making is what is called a "multistakeholder model." This decentralized governance model places individuals, industry, non-commercial interests and government on an equal level. Unlike more traditional, top-down governance models, where governments make policy decisions, the multistakeholder approach used by ICANN allows for community-based consensus-driven policy-making. The idea is that Internet governance should mimic the structure of the Internet itself – borderless and open to all.

While the ICANN Board of Directors has the ultimate authority to approve or reject policy recommendations, Supporting Organizations (SOs) are responsible for developing and making policy recommendations to the Board. Advisory Committees (ACs) advise the ICANN Board and, in certain cases, can raise issues for policy development. The SO/ACs are described in more detail later in this booklet.

ICANN staff is responsible for executing and implementing policies developed by the ICANN community and adopted by the ICANN Board.

The ICANN Ombudsman is an independent, impartial and neutral person contracted to ICANN, with jurisdiction over problems and complaints made about decisions, actions or inactions by ICANN, the Board of Directors, or unfair treatment of a community member by ICANN staff, Board or a constituency body.

The Nominating Committee is a team of community volunteers responsible for the selection of eight ICANN Board members, and portions of the At-Large Advisory Committee, the Country Code Names Supporting Organization and the Generic Names Supporting Organization.

What Happens at an ICANN Meeting?

ICANN holds three international public meetings each calendar year in different regions of the globe. One meeting each year is also the organization's annual general meeting, during which new Board members take their seats.

Usually comprised of more than 200 different sessions, the week-long meeting is a focal point for individuals and representatives of the different ICANN stakeholders (either attending in-person or participating remotely) to introduce and discuss issues related to ICANN policy. In most cases anyone may speak, but in a few cases you may need to be a member of a particular group. If you are uncertain of the rules during a session, simply ask the session leader if you may speak.

Meetings are open to everyone and registration is free, but you are responsible for your own travel and lodging. ICANN offers limited financial assistance to members of its Supporting Organizations and Advisory Committees. Also, there is a Fellowship program for selected candidates from developing countries who otherwise could not afford to attend in-person.

If you cannot physically attend a meeting, ICANN offers a variety of services to ensure that the power of participation is just a click away. Virtual meeting rooms are available for nearly all sessions with access to meeting materials, a chat room and for larger or general sessions, video and/or audio streaming and live transcription.
Learn more at http://meetings.icann.org/remote-participation

Though English is the main language at ICANN meetings, translation, scribing and interpretation are available at certain sessions. Many documents are made available in Arabic, Chinese, French, Russian and Spanish.

Each meeting has a dedicated web site with a frequently updated meeting schedule, venue map, information on the local area and social events.

Public Comment Periods at ICANN
A vital element in ICANN's processes is the opportunity for public comment on each substantial piece of work before it is considered for approval. These topics can be operational (such as budget or strategic planning), technical (such as security reports and recommendations) or policy-oriented (such as Bylaw changes).
The following principles guide the public comment process:
- Each item posted for public comment is available for a minimum of 21 days.
- If comments are received, then at the close of the comment period, a reply period begins, lasting a minimum of 21 days.
- If no substantive comments are received during the comment period, then there will be no reply period.
- During the reply period, participants should address previous comments submitted; new posts concerning the topic should not be introduced. When constructing replies, contributors are asked to cite the original poster's name, comment date, and any particular text that is pertinent.

You can find a list of all topics open for public comment on a dedicated public comment page (http://www.icann.org/en/news/public-comment). The page includes links to relevant announcements, documents, comment locations, and reference sources with full descriptions and background information.

After the comment period is closed, staff publishes a comment summary report that is archived along with all public comment documentation and comments received.

ICANN Government Advisory Committee (GAC) Info

What is the GAC?
The GAC is an advisory committee to ICANN, created under the ICANN ByLaws. It provides advice to ICANN on public policy aspects of ICANN's responsibilities with regard to the Internet Domain Name System (DNS). According to its Operating Principles, the GAC serves as a forum for the discussion of government and other public policy interests and concerns including, among other things:

- secure, reliable and affordable functioning of the Internet, including uninterrupted service and universal connectivity;
- the robust development of the Internet, in the interest of the public good, for government, private, educational, and commercial purposes, worldwide;
- transparency and non-discriminatory practices in ICANN's role in the allocation of Internet names and address;
- effective competition at all appropriate levels of activity and conditions for fair competition, which will bring benefits to all categories of users including, greater choice, lower prices, and better services;
- fair information practices, including respect for personal privacy and issues of consumer concern; and
- freedom of expression.

The GAC is not a decision-making body. It advises ICANN on issues that are within ICANN's scope.

GAC advice has a particular status under the ICANN ByLaws. Its advice must be duly taken into account by the ICANN Board, and where the Board proposes actions inconsistent with GAC advice it must give reasons for doing so and attempt to reach a mutually acceptable solution.

The GAC appoints a non-voting liaison to the ICANN Board. This is normally the GAC Chair.

Who are the GAC's Members?

The GAC elects a Chair and Vice Chairs from its membership. The current GAC Chair is Mr Thomas Schneider from Switzerland, and the Vice Chairs are from Argentina, Spain, Namibia, Thailand and Turkey. Elections for the Chair take place at the last meeting every two years, with the next election in late 2016, and for the vice chairs at the last meeting every year.

GAC membership consists of national governments and distinct economies recognized in international fora; and, usually in an observer capacity, multinational governmental and treaty organisations and public authorities (including all the UN agencies with a direct interest in global Internet governance such as the ITU, UNESCO and WIPO). Observers participate fully in the GAC and its Committees and Working Groups but do not have voting rights. There are currently 137 GAC Members and 30 Observers.

Why does ICANN have a Governmental Advisory Committee?

ICANN is a multi-stakeholder entity in which governments need to participate alongside the domain names industry, the technical community, business and non-commercial users, and civil society. The GAC was established in 1999, in parallel with ICANN's first public meetings, and has operated continuously since then.

ICANN looks to the GAC for advice on public policy aspects of specific issues for which ICANN has responsibility. This is an important dimension of ICANN's work.

How does the GAC operate?

The GAC determines its own operating procedures and these are set out in the GAC Operating Principles. GAC face-to-face meetings are held in conjunction with ICANN meetings, which currently occur three times a year.
Advice from the GAC to ICANN is determined on the basis of consensus. Advice is conveyed to the ICANN Board, usually in the form of a communiqué issued at the end of each GAC meeting. Each communiqué and the minutes of GAC meetings are made available online.

The GAC works inter-sessionally on priority issues, usually via teleconferencing. In addition, working groups are used to focus on particular areas such as working methods and issues for future gTLDs. The Public Safety Working Group (PSWG) is the first permanent Working Group of the GAC. There may also be in the near future a Working Group on Human Rights.

The work of the GAC is supported by a dedicated Secretariat provided by ACIG (an independent consulting firm) and by ICANN staff.

What are the benefits of GAC membership?

The Internet domain name system is a key part of critical Internet infrastructure for the global digital economy. Government and IGOs who participate through the GAC benefit from:

- The opportunity to provide advice directly to the ICANN Board on public policy aspects of the operation of the Internet domain name system.
- Contributing at an early stage of ICANN's policy development processes to ensure consistency with laws and public interest.
- Access to face to face meetings and online discussion with other GAC members and observers, including national governments and inter-governmental organisations, which inform development of GAC advice.
- Access to relevant subject matter experts within the GAC and across ICANN, enabling GAC members to remain informed about technical innovation in the domain name system and its future evolution.
- Support from a professional full-time Secretariat.
- Substantive policy outcomes, including the below;

GAC Achievements

- The 2007 new principles for generic top level domains (gTLDs)
- New gTLDs scorecard, which was important to the new gTLDs program and widely hailed as a major success and model for the future
- ICANN's acceptance of safeguards for new gTLDs to reflect law enforcement and consumer protection concerns.
- WHOIS principles, including bringing law enforcement to the ICANN table to address cybercrime
- Maintaining security and stability of the DNS
- Delegation and administration of country code domains (ccTLDs)

Structural and process outcomes, including

- Greater accountability and transparency of all areas of ICANN (including the GAC itself)
- Liaison with the ICANN Board, through the GAC Chair's membership and a formal register of GAC advice and actions taken
- Cross-community activities between GAC and ICANN policy-making bodies such as those dealing with generic and country-specific top level domain names.
- Operation of a travel support program to assist developing countries to participate in GAC meetings.
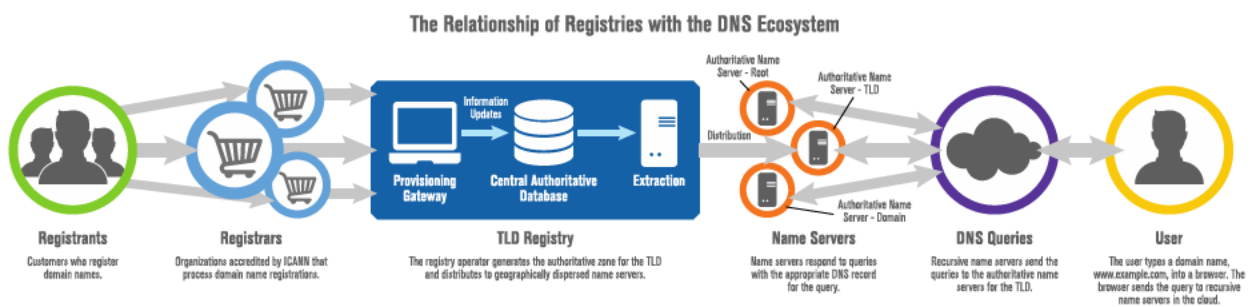
Registrars and Registries

Two important groups of players in the day-to-day working of the internet are the registries and the registrars.

The **registries** (also called "registry operators" or "sponsors") bear responsibility for operating a "top-level domain" (TLD). The TLD is the right-most label in a domain name (e.g. www.icann.org); all websites hosted under a TLD are part of that TLD's registry, which maintains a list of the domain names within the TLD. There are two types of TLDs:

- TLDs with two letters which have been established for over 240 countries and external territories and are referred to as "country-code" TLDs or "ccTLDs." A list of all ccTLDs can be found here: http://www.iana.org/cctld/cctld-whois.htm

- TLDs with three or more characters are referred to as "generic" TLDs, or "gTLDs." For a full list of gTLD registries, please see here: http://www.icann.org/en/resources/registries/listing

The **registrars** sell domain names to the public, either directly or through resellers, and register the (new) owner of the domain (the "registrant") in the appropriate registry. They have a contractual relationship with ICANN, who accredits them; with the registry for which they are authorized to sell domain names; and with the person or entity registering for the use of a domain name, the registrant. For a list of all current ICANN-accredited registrars, please see http://www.internic.net/regist.html. For more information on registrars, please see here: https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en.

The pictures below (source: Spec11 Draft Framework for Registry Operators to Respond to Security Threats) illustrate the relationships between ICANN, registries, registrars and end users:

The Relationship of Registries with the DNS Ecosystem
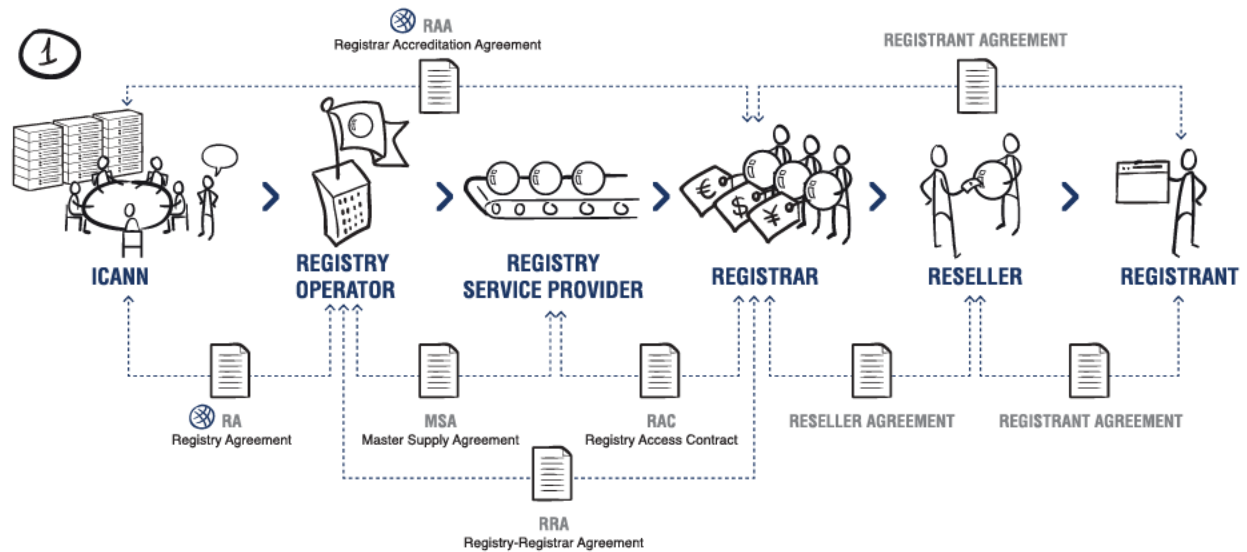
Given the key role of registries and registrars in preventing and combating abuse of domain names, activities aimed at ensuring consideration of public safety interests have focused on inspiring registries and registrars to take a more proactive stance against such abuse. A key step in this process was the adoption of law enforcement recommendations for the new, 2013, Registrar Accreditation Agreement.

General ICANN Links

What is ICANN?
https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf

General WHOIS Information:
http://whois.icann.org/

WHOIS Inaccuracy Reporting:
https://forms.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form

http://whois.icann.org/en/whois-complaints

Contract Compliance
General Information: https://www.icann.org/resources/pages/compliance-2012-02-25-en

How to file Registrar Violation of 2013 RAA:
https://www.icann.org/resources/pages/complaints-2013-03-22-en

Government Advisory Committee (GAC)
https://gacweb.icann.org/display/gacweb/GAC+Representatives
https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee

Registrar Accreditation Agreement (RAA)
2013 RAA: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

LE Recommendations and Changes to 2009 RAA: https://www.icann.org/public-comments/proposed-raa-2013-04-22-en

New gTLDs
http://newgtlds.icann.org/en/

Internationalized Domain Names (IDN)
General Information: https://www.icann.org/resources/pages/idn-2012-02-25-en
IDN Variants (confusability): https://www.icann.org/resources/pages/variant-tlds-2012-05-08-en
ICANN Final IDN WHOIS Report: http://gnso.icann.org/en/issues/ird/final-report-ird-wg-06mar12-en.pdf

Law Enforcement Participation

INTERNET GOVERNANCE

Law Enforcement History of Internet Governance Efforts

2003

- ICANN Montreal: FBI and US Department of Justice (DOJ) participate and attend WHOIS Panel – privatization of WHOIS is discussed. DOJ articulates need for continued open and accurate WHOIS for international law enforcement (LE) investigations.

2004

- ICANN Cape Town: FBI attends ICANN to track ongoing WHOIS debate and ensure LE input is provided.

2005

- ICANN Mar del Plata: FBI attends ICANN to monitor WHOIS developments.

- ARIN: FBI, Royal Canadian Mounted Police (RCMP) and DOJ participate at American Registry for Internet Numbers (ARIN) meeting in Orlando (April 2005) for WHOIS Policy discussion on limiting WHOIS information. Because of LE opposition, restrictive ARIN policy is rejected.

- ICANN Luxembourg: FBI in conjunction with Government Advisory Committee (GAC), sponsored and coordinated a LE panel regarding LE use of WHOIS and the need for open and accurate WHOIS for international LE. Presentations made by UK Home Office, Australian Federal Police, Spanish Guardia Civil, Malawian National Police, and Interpol.

2006

- ICANN Marrakesh: US Federal Trade Commission (FTC), Japan, and Netherlands (OPTA) civil LE agencies make presentations to the GAC on importance of the WHOIS for consumer protection. UK Serious Organised Crime Agency (SOCA) and FBI in attendance.

- ICANN Sao Paulo: RCMP attend their first ICANN meeting.

2007

- ICANN Lisbon: GAC with LE coordination publish "Legitimate Uses of WHOIS," which still stands as GAC WHOIS Policy.

2008

- ICANN Paris: FBI organizes first LE Day at ICANN. This first all-day LE session was an introduction for LE to the importance of ICANN, and how LE can interact and participate at ICANN meetings.

    o In attendance were LE representatives from: UK (SOCA), France (National Police), South African Police Service, RCMP, Japanese National Police, Lithuanian National Police, US (FBI, USSS), Dutch High Tech Crime Centre, Spain (Guardia Civil), and Cyprus (National Police)

- September 2008 - Réseaux IP Européens Network Coordination Centre (RIPE NCC) –European LE and FBI participate at RIPE NCC's biannual "Government Roundtable" meeting in Amsterdam. First time LE gathers at RIPE NCC.

2009

- ARIN Government Working Group (AGWG) formed: Attendees from 15 Canadian and US government and LE agencies. Goal of AGWG is to inform LE on ARIN policies that impact LE and participate in drafting appropriate policies to ensure investigative capabilities are maintained. AGWG continues to meet consistently in US and Canada in preparation for ARIN meetings. AGWG has successfully supported and rejected ARIN polices that were of importance to LE.

- Second RIPE NCC Government Roundtable Meeting (February 2009). European LE in attendance. UK SOCA consistently attends RIPE NCC meetings from this point forward.

- ICANN Mexico: Second LE Day. In attendance were Mexican National Police, FBI, SOCA, and RCMP.

- LACNIC Meeting Panama: LE from Brazil, Costa Rica, Uruguay, and Nicaragua meet to establish LACNIC Government/LE Working Group

- ICANN Seoul: *FBI/ SOCA with support of international LE introduce and present "Law Enforcement Due Diligence Recommendations for ICANN" (LE Recommendations) to the GAC.* http://gnso.icann.org/en/issues/raa/raa-improvements-proposal-final-report-18oct10-en.pdf *(See Appendix G)*

2010

- AfriNIC: African Network Information Center (AFRINIC) Government Working Group with LE participation is created. Representatives from Seychelles, Kenya, Nigeria, Mauritius, South Africa, Benin, and Tunisia attend.

- ICANN Nairobi: SOCA presents GAC with written endorsements of LE Recommendations from Interpol, Council of Europe and G8.

- ICANN Brussels: International LE meet with GAC. ***GAC formally endorses LE Recommendations and forwards to ICANN Board of Directors as formal GAC advice.*** Interpol, G8, Messaging Anti Abuse Working Group (MAAWG), and London Action Plan all endorse in writing. In attendance:

  - Quebec Provincial Police; German Federal Criminal Police (BKA); Japanese National Police; Belgian Federal Police; European Commission (DG Home) Europol; Indonesian Ministry of Communication and Information Technology; Brazilian Federal Police; New Zealand Police; Netherlands (High Tech Crime Centre and OPTA); Switzerland Federal Intelligence Service; UK (SOCA and Children's Charities Coalition on Internet Safety); and USA (FBI, US National Center for Missing and Exploited Children (NCMEC), Drug Enforcement Administration (DEA), US Federal Trade Commission (FTC), and Secret Service)

- LE-Registrar/Registry Meeting (September 2010) in Washington DC: International LE meet with gTLD registrars and registries to discuss LE Recommendations. Full day meeting focused on discussion of Recommendation and their implementation.

2011
- LE-Registrar/Registry Meeting at European Commission offices in Brussels, Belgium (February 2011): International LE meet for 2-day meeting to discuss how registrars can implement LE Recommendations. Registrars publish document of agreement to a number of LE Recommendations.

- ICANN San Francisco: LE proposes Statement of Commitment by registrars based on Brussels meeting. Registrars do not agree to sign or move forward. Interpol, UK, Canada and US in attendance.

- Establishment of North American Carrier Grade NAT (CGN) Working Group (June 2011, Washington, DC): Canadian and US LE (Europol joins in 2012) organize the first of 9 meetings with government, ISPs, vendors and content providers to address CGN lack of attribution challenge. Subsequent meetings are held in September and October 2011; January, May and September 2012; March and September (Europol) in 2013; and the final meeting in January 2014. CGN Working group produced one IETF

RFC (6302) and one IETF Internet Draft on Deterministic Logging. In addition, legislation was drafted but not forwarded.

- ICANN Singapore: No progress on LE Recommendation despite LE renewed language and proposals. UK, US, Singapore, Interpol and Canada in attendance.

- ICANN Dakar: GAC demands actions on LE Recommendations due to lack of progress. *New ICANN Chairman of the Board, Steve Crocker, orders ICANN to begin immediate negotiations with gTLDs registrars for the drafting of a new Registrar Accreditation Agreement (RAA)* with the inclusion of LE Recommendations. Interpol, US, UK and Canada attend.

2012
- ICANN Costa Rica: LE Day; Representatives from Australia, Brazil, UK SOCA, Interpol, Canada, US Department of Justice (DOJ), FBI , DEA , Homeland Security Investigations (HSI) and FTC attend.

- LE/ICANN/Registrars begin negotiations on new RAA with LE Recommendations (February 2012)

- ICANN Prague: SOCA organizes LE Day – UK, Spain, France, Czech Republic, Netherlands, Europol, Canada and US attend. First formal LE meeting with ICANN Security and Stability Advisory Committee (SSAC). SSAC will present at LE Days consistently from this meeting on.

- ICANN Toronto: RCMP/Quebec Police organize LE Day with attendance from Canadian local and provincial LE, Germany, US and UK. First meeting with Europol EC3.

2013
- ICANN Beijing: *Introduction of new gTLD GAC Safeguards*. LE Day (China, Interpol, Europol, UK and US). Europol and FBI present to GAC outstanding issues with RAA.

- ICANN Durban: *ICANN signs new 2013 RAA with LE Recommendations incorporated. Registrars have until January 1, 2014 to sign.*

- ICANN Buenos Aires: LE Day with Argentine LE and government officials. US, Europol and Interpol attend.

2014

- ICANN Singapore: Interpol organizes LE Day. Due to lack of progress on GAC new gTLD safeguards, LE submits additional GAC advice to ICANN Board of Directors.

- ICANN London: Europol organizes LE Day with heavy European participation. Further GAC Safeguard advice on new gTLDs.

- ICANN Los Angeles: FBI organizes LE Day with public and private sessions. Attendance includes Europol, Interpol, Argentina BAMP, Korea National Police, Quebec Provincial Police, UK Metropolitan Police and European Commission.

2015

- ICANN Singapore: Public Safety Working Group (PSWG) formally created as a sub group of the GAC.

- ICANN Buenos Aires: PSWG holds first official meeting. GAC formally endorses the PSWG Terms of Reference.

- PSWG holds second official meeting in Washington DC (September 2015). In attendance include Interpol, Europol, FBI, OAS, US FTC, Switzerland MELANI, RCMP, US DOJ, European Commission, US FDA, UK NCA, International Association of Chiefs of Police (IACP), UK MHRA, IRS, HIS and DEA.

- ICANN Dublin: PSWG hold public forum to summarize current activities to the community prior to formally presenting in front of the GAC. Closed session also occurs with international LE members of the PSWG to discuss working plan and way forward. Registrars organize meeting with LE to discuss upcoming "uniform responses to LE requests" publication.

- October 2015: PSWG submits letter to Numbering Resource Organization (NRO) asking for WHOIS accuracy requirements for IP WHOIS.

Fadi Chehade Letter to Public Safety Working Group

The Internet Corporation for Assigned Names and Numbers

ICANN

23 May 2014

SSA Robert Flaim, FBI
Cap. Frederick Gaudreau, Francopol
Mrs. Laureen Kapin, FTC
Mr. Richard Leaning, Europol
Mr. Kimmo Ulkuniemi, Interpol

Re: Participation of law enforcement and consumer protection agencies in ICANN's multistakeholder process

Dear Mrs. Kapin and Messrs. Flaim, Gaudreau, Leaning and Ulkuniemi:

Thank you for your letter of 14 May 2014 regarding the participation of the law enforcement and consumer protection agencies in ICANN's multistakeholder environment. I am so pleased to know that you all have begun discussions within your own agencies to elicit support and identify concerns.

We look forward to the discussions that will take place on this important matter during and after ICANN's 50th Public Meeting in London in June. Our team will continue to work with you to make progress on this front, reflecting the substantial interest that the organization has had and maintains regarding public safety and consumer protection issues.

I will be happy to receive your proposal on how your agencies can participate at ICANN in a more institutionalized manner. And I will also be happy to bring your proposal to the Board of Directors for further, open discussions.

I count on, and value greatly, your continued participation in ICANN's multistakeholder process.

Warm Regards,

Fadi Chehadé
President & CEO

cc: Steve Crocker

Public Safety Working Group (PSWG)

Introduction

The GAC has a mandate to ensure that public policy interest, including safety and security, are taken into account in ICANN policies, procedures and day-to-day operations. To fill this mandate with life, law enforcement and consumer protection bodies have been involved in the work of the GAC and ICANN as a whole for more than a decade, as outlined in the previous section. The ICANN board and the GAC officially recognized this work and gave it an institutional framework in 2015 by creating a Public Safety Working Group (PSWG) as a permanent sub-group of the GAC.

The sections below contain the Terms of Reference of the PSWG as well as some examples of recent comments provided in various consultation processes on policies with an impact on public safety concerns.

Public Safety Working Group Terms of Reference

Established: Feb 2015, ICANN52 Singapore
Lead: Alice Munyua (African Union Commission)
Mailing list: gac-pswg@icann.org (please email gacsec@gac.icann.org if you wish to subscribe to the mailing list)

These are the Terms of Reference for the Public Safety Working Group (PSWG), an internal working group of ICANN's Governmental Advisory Committee (GAC).

The focus of the PSWG will be on those aspects of ICANN's policies and procedures that implicate the safety of the public.

Objectives
The GAC's PSWG objectives include, but are not limited to, the following:

7. Assessing whether and seeking to ensure that the Domain Name System (DNS) and domain name registrations are not used to propagate, enhance, or further, unlawful activity, abuse, consumer fraud, deception, or malfeasance, and/or violations of law;
8. Supporting the ability of public safety organizations to investigate, prevent, attribute, and disrupt unlawful activity, abuse, consumer fraud, deception or malfeasance, and/or violations of national law that involve the DNS and domain name registrations;
9. Cooperating with ICANN's advisory committees (including the RSSAC, SSAC), supporting organizations (including the GNSO, ASO, ccNSO), and community, to ensure multi-stakeholder support and cooperation, in advancing public safety policies, recommendations, and advice;

10. Participating in applicable ICANN working/study groups to promote a shared understanding of the potential effects such groups' work and recommendations will have on public safety;

11. Continuously assessing whether ICANN has responsive and timely mechanisms to develop and enforce ICANN contractual obligations with gTLD registries and registrars, (*i.e.*, Registrar Accreditation Agreement, Registry Agreement); and

12. Addressing work streams, policies, and studies that are brought forth at ICANN that affect public safety.

Working Group Members

The GAC's PSWG Co-Chairs will be Ms Alice Munyua, African Union Commission and Mr Wanawit Ahkaputra, Thailand.

All GAC representatives and observers are welcome to join the PSWG. The primary members of the PSWG, however, are expected to be representatives from national and/or provincial/state government consumer protection, civil and criminal law enforcement, and other agencies responsible for the welfare and protection of its citizens who:

1. Demonstrate knowledge or expertise about Internet governance, the DNS and the Internet; and

2. Commit to participate in the activities of the working group on a consistent basis, either in-person or remotely by teleconference, email, etc.

GAC members are therefore asked to identify and nominate such representatives to participate actively in the work of the PSWG.

This is permissible under GAC Operating Principle 27, which states: "The Chair may call for the creation of Committees and Working Groups to address matters that relate to concerns of governments and where they may affect public policy issues. Accredited representatives may designate advisers to serve on such committees."

All participants will be listed in the working group's online workspace, within the members-only section of the GAC website.

The working group will be assisted and supported by the ACIG GAC Secretariat and the ICANN GAC Support team.

Deliverables and Timeframes

The PSWG will hold its first official meeting at the next ICANN meeting in Buenos Aires in June 2015. In addition, the PSWG will:

- introduce the PSWG and its mission to all relevant ICANN groups and constituencies;
- research, draft, and submit to the GAC, advice on subjects that may affect public safety;

- consult with operational security experts from industry and other sources on cyber-security issues relating to the DNS; and
- develop a range of best practices, support, advice, and assistance consistent with the working group's objectives.

Current areas of interest, as of **May 2015**, for the PSWG (which may evolve/change) include:
- WHOIS: ICANN currently has approximately 15 separate tracks concerning WHOIS, (i.e., accuracy project, privacy and proxy services accreditation, Expert Working Group report, etc.;
- Specification 11 of gTLD Registry Agreement
- New Public Interest Commitment on Security Threats
- Contractual Compliance;
- Implementation of new gTLDs;
- Internationalized Domain Names.

The PSWG will support the GAC on public safety developments, opportunities and challenges. Accordingly, the PSWG Chair will update the GAC about the PSWG's activities at each face-to-face GAC meeting. Members of the PSWG will be responsible for maintaining and coordinating with the Chair on PSWG initiatives, studies and publications. An email list will be established to aid the work of the group. Details of how to subscribe to the email list will be published on the web page of the working group.

Working methods

The working group will aim to act by consensus. If members of the PSWG cannot reach full consensus, the WG Chair will convey the full range of views of the members.

The PSWG may, at its discretion, publish an interim review and analysis of the topics it considers relevant to its work, in the form of Position Paper or a Statement based on the consensus view of the members of the working group.

The draft text will be submitted to the GAC plenary for comment, and may also be published with a view to seeking comments or input from the wider ICANN community and/or relevant stakeholders outside the community.

Any such draft Position Paper or Statement must clearly state that it is produced by an internal GAC Working Group and does not represent a consensus GAC view.

After reviewing the responses to the draft Position Paper or Statement, the working group may seek formal GAC endorsement or support for the document. In the event that the GAC does not support or endorse a Position Paper or Statement, the working group may, at its discretion, reconsider and/or revise the Position

Members list

GAC member/ Observer	Contact
African Union Commission	Alice Munyua (Chair)
Argentina	Olga Cavalli Ezequiel Sallis, Buenos Aires Police
Australia	Annaliese Williams Adrian Norris Glyn Lewis
Belgium	Jean-Philippe Moiny Fernand Van Gansbeke Ruben Verstraete
Canada	Andrea Todoran Maury Medjuck, Royal Canadian Mounted Police Doug Ross, Royal Canadian Mounted Police Lise Landry-Morson, Competition Bureau Andre Leduc, Industry Canada Pamela Miller Christian Dumas Erin Dorgan
Council of Europe (CoE)	Lee Hibbard
Columbia	Claudia Ximana Bustamente
China	Guo Feng
Dominica, Commonwealth of	Thomas Benette
Egypt	Manal Ismail
European Commission	Megan Richards Cathrin Bauer-Bulst Cristina Monti Michael Palmer
EUROPOL	Gregory Mounier
Germany	Sabine Meyer Hubert Schoettner Eva Petsch
India	Ajay Kumar

GAC member/ Observer	Contact
International Association of Chiefs of Police (IACP)	James Emerson
Italy	Rita Forsi Maura Gambassi
INTERPOL	Adrian Eduardo Acosta Kimmo Ulkuniemi
Italy	Maura Gambassi
Japan	Shuji Yamaguchi
Morocco	Redouane Houssaini
Netherlands	Thomas de Haan
Niue	Pär Brumark
OAS	Belisario Contreras Kerry-Ann Barett
Senegal	Amadou Ly
Switzerland	Jorge Cancio Adrian Koster (Advisor)
Thailand	Wanawit Akhuputra Pitinan Kooarmornpatana Artthawit Hung Panus Rattakitvijun Na Nakorn
Trinidad and Tobago	Tracy Hackshaw Joseph Dale, Trinidad and Tobago Police
Ukraine	Oleksandr Tsaruk
United Kingdom	Mark Carvell Jonathan Flaherty Nick Shorey Stephen Truick Will Metters John Carr
United States	Suzanne Radell Ashley Heineman Laureen Kapin, Federal Trade Commission (FTC) Daniel Burke, Food and Drug

GAC member/ Observer	Contact
	Administration (FDA)
	Robert Flaim, Federal Bureau of Investigation (US DO)
	Ella Smallwood, Federal Bureau of Investigation (FBI)
	Iranga Kahangama, Federal Bureau of Investigation (FBI)
	Mike Freeman, Drug Enforcement Agency (DEA)
	Man Tse, Homeland Security Investigations
	Mark Hendersen, Internal Revenue Service (IRS)
	Amy J Sanbury, US Department of Justice (DOJ)
	Thomas Walden, US Department of Justice (DOJ)
	Peter Roman, US Department of Justice (DOJ)
	Carmen Alvarez, US Department of Justice (DOJ)
	Herbert Freeman, US Department of Justice (DOJ)
	James Emerson, Law Enforcement Online
Venezuela	Jesus Rivera

Examples of PSWG work

1. Comments on Privacy/ Proxy Services Accreditation

Privacy and proxy services are for individuals and entities who wish to keep certain information from being made public via WHOIS.

There are two general types of these services:

- A *Privacy Service* lists alternative, reliable contact information, like an address or phone number, in WHOIS while keeping the domain name registered to its beneficial user as the registrant.
- A *Proxy Service* registers the domain name itself and licenses use of the domain name to its customer. The contact information of the service provider is displayed rather than the customer's contact information. The proxy service is responsible for providing accurate contact information adequate to facilitate timely resolution of any problems that arise in connection with the domain name. The proxy service accepts liability for harm caused by wrongful use of the name unless it promptly discloses the identity of the licensee to a party providing reasonable evidence of actionable harm.

Privacy and Proxy Services offered by Registrars or their affiliates are subject to additional obligations. These Privacy and Proxy Providers must disclose their Service Terms, publish an Abuse of Point Contact and meet Escrow Obligations.

Privacy and Proxy Services are among the least well-developed policy areas. A Policy Development Process is currently ongoing to provide policy recommendations on how to design an accreditation process for privacy and proxy services. For this purpose, a Privacy & Proxy Services Accreditation Issues ("PPSAI") Working Group was chartered by the Generic Names Supporting Organisation (GNSO) Council. It published an initial report on accreditation issues for public comments in May 2015 (the Initial Report, public comments received and the staff report of the public comments can be viewed at https://www.icann.org/public-comments/ppsai-initial-2015-05-05-en). The following comments, prepared by the PSWG, were submitted on behalf of the GAC.

The PPSAI Working Group has published a draft final report on 7 December 2015, available at http://gnso.icann.org/en/issues/raa/ppsai-final-07dec15-en.pdf.

GAC Public Safety Working Group (PSWG) Comments to Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process

After review of the Initial Report on the Privacy & Proxy Services Accreditation Issues
Policy Development Process, the PSWG provides the following comments and recommendations:

Distinction between Commercial and Non-Commercial Users:

- In order to promote transparency and consumer safety and trust, the PSWG recommends against permitting websites actively engaged in commercial transactions – meaning the collection of money for a good or service – to hide their identities using Privacy/Proxy (P/P) Services.[1] This includes domains used for websites that directly collect payment data, as well as for sites that promote a transaction but directly link to other sites that execute the transaction. The public is entitled to know the true identity of those with whom they are doing business. Indeed, many nations have laws specifically mandating such transparency in commercial and business transactions.

- P/P services should only be permitted for those domains that are not actively conducting business transactions, as detailed in the above. Any person or entity that engages in commercial transactions invites the public to trust them with their funds and sensitive financial account information. Hence, any privacy interest should be balanced with the public's right to know the true identity of those with whom they are doing business.

Transparency and Accountability:

- The PSWG supports the conclusion that ICANN should ensure transparency by publishing and maintaining a publicly accessible list of all accredited P/P service providers, with all appropriate contact information. Registrars should provide a web link to P/P services run by them or their Affiliates, and P/P service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program.

---

[1] Any definition of "commercial transactions" and limitations on use of P/P services should not apply to registrants whose sites are supported by advertising (and thus arguably "commercial"), but are not actively engaged in financial transactions.

- The PSWG supports the conclusion that a "designated" rather than a "dedicated" point of contact will be sufficient for abuse reporting purposes and a designated point of contact should be "capable and authorized" to investigate and handle abuse reports, consistent with RAA Section 3.18.

- The PSWG agrees that proxy and privacy services should be treated equally for the purpose of accreditation process.

- The PSWG concurs with the P/P WG preliminary conclusion that domain name registration involving P/P service providers should be clearly labelled as such in the WHOIS.

- The PSWG recommends that P/P customer data should be validated in compliance with the RAA Cross-Validation requirement, pursuant to RAA WHOIS ACCURACY PROGRAM SPECIFICATION, paragraph 1 "… Registrar will, with respect to both WHOIS information and the corresponding customer account holder contact information related to such Registered Name…" validate the information provided.

- PSWG believes that proxy/privacy services should continue to be required to publish their relevant terms of service and to abide by those published terms (as currently provided in the Interim Specification to the 2013 RAA).

<u>Definition of Law Enforcement</u>

- "Law Enforcement Authority" is defined as "law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the privacy or proxy service provider is established or maintains a physical office." To the extent this definition could be viewed as suggesting that P/P service providers need only respond to law enforcement authorities within their own jurisdiction, the PSWG urges the P/P Working Group to consider revising this definition. Malicious conduct involving domains often takes place across borders and the definition of law enforcement should recognize the multi-jurisdictional aspects of investigative and enforcement activities in order to promote protecting the public no matter where they are located. If such revisions are made, the Working Group should consider a requirement that a P/P service consult with its local law enforcement authorities in the event it receives a request from a foreign authority (to ensure that the local authorities believe that the request is a proper request from a recognized foreign authority).

<u>Confidentiality of Law Enforcement (including Consumer Protection) Requests</u>

- Although the Initial Report did not reflect an agreement on the issue of whether P/P Service Providers should disclose requests from law enforcement, the PSWG appreciates the Initial Report's recognition of the "need for confidentiality in relation to an ongoing LEA investigation." Section 1.3.2 at p. 15. Law Enforcement Agency and Consumer Protection Agency (collectively "LEA") requests are directly related to ongoing investigations. Notifications to customers, who may be the alleged criminal or violator, could threaten not only the effectiveness of the investigation but could also threaten the safety of individuals. Accordingly, the PSWG urges P/P Working Group to require P/P Service Providers to keep LEA requests confidential as required and/or permitted by local laws.

- Requests by LEAs are directly related to sensitive investigations involving violations of the law. Many malware and other seemingly less critical violations have hidden connections to more malevolent criminal enterprises. Given the variety of subject areas for LEA investigations, it would be virtually impossible to confine the topics of potential investigations into select categories for the purposes of P/P Services. If a P/P provider were to provide notice of a LEA investigative request to the target of the request, remedies for such disclosure by the P/P provider would be determined by the respective national, state, provincial, or other governing laws.

Conclusion

Public safety authorities, including law enforcement and consumer protection agencies, play a vital role in responding to incidents of crime, victim distress, potential harm, and in worst case scenarios, victim identification. To the extent, privacy services are used to hide the actors responsible for malicious activities or obscure other pertinent information, there must be reasonable mechanisms in place for public safety authorities to unmask bad actors and obtain necessary information. We urge the P/P Working Group to take into account the law enforcement need to obtain information cloaked by privacy services in order to continue to protect the public from malicious conduct that involves internet domains.

2. Invitation for joint workshop with the Regional Internet Registries

Regional Internet Registries (RIRs) are nonprofit corporations that administer and register Internet Protocol (IP) address space and Autonomous System (AS) numbers within a defined region. RIRs also work together on joint projects. There are five of them:

Registry	Geographic Region
AFRINIC	Africa, portions of the Indian Ocean
APNIC	Portions of Asia, portions of Oceania
ARIN	Canada, many Caribbean and North Atlantic islands, and the United States
LACNIC	Latin America, portions of the Caribbean
RIPE NCC	Europe, the Middle East, Central Asia

A key role of the RIRs is the administration of IP address space allocation, including the maintenance of an IP version of the Whois, a database which provides the IP Address owner's information. The IP Whois information contains data such as who allocates the IP (ie. ARIN, APNIC, RIPE, etc.), if the IP Address is allocated, IP Address contact information, how many IP addresses are in the block or blocks assigned to the owner of the IP, and more. Accuracy of the IP Whois has been a concern, and the PSWG is now reaching out to the RIRs to try to find common solutions for improving the reliability of IP Whois. In a first step, a joint workshop at ICANN55 in Marrakech is planned; please see below for the workshop invitation.

For more information on RIRs, please see
https://www.arin.net/knowledge/rirs.html.

Work Plan - GAC Public Safety Working Group

What (Task Name / Description)	Who	By When	Stakeholders	Output (ie a Decision or Document)
1. PSWG PROCESSES, MEETINGS & OUTREACH				
Terms of Reference for PSWG	PSWG members	Completed, endorsed by GAC at the BA meeting	Law Enforcement Agencies (LEAs), consumer protection agencies and other public safety agencies	PSWG Terms of Reference endorsed by the GAC in Buenos Aires
Second face to face PSWG meeting	PSWG members	Completed, 10 Sept 2015	Public safety agencies	Report on GAC Public Safety Working Group (PSWG) meeting: 10 September 2015, Washington DC
Public Meeting of the PSWG at ICANN54	PSWG members & all interested	Completed, 19 Oct 2015	LEAs, consumer protection agencies and other public safety agencies	Report on GAC Public Safety Working Group (PSWG) meeting of 19 October 2015, Dublin
PSWG meeting, 28 January 2016, Brussels	EC, ICANN	January 2016	Public safety agencies	Report on meeting.
Local public safety agencies meeting at ICANN 55	AOS, ICANN	Ongoing – ICANN Marrakesh	Public safety agencies	Meeting of local public safety agencies at ICANN55.
Outreach to members from developing countries and others	AUC, OAS, GAC, ICANN (Fellowship Program)	Ongoing and long term	Public safety agencies, esp. in developing regions	New PSWG members (to be confirmed).
Harmonizing international requests to registrars and registries (Outreach)	PSWG and respective government officials.	Ongoing and long-term	Public safety agencies	Request templates (to be confirmed).
2. WHOIS / DIRECTORY SERVICES				
Registrar Accreditation Agreement (RAA): WHOIS Accuracy Program Specification Review	PSWG members	Completed, August 2015	Public safety agencies, registrars, ICANN	GAC comments on the review of the WHOIS Accuracy Specification
Privacy and Proxy Accreditation Services of the gNSO GNSO PPSAI Working Group	PSWG	Completed, August 2015	Public safety agencies, P&P service providers, ICANN	GAC Comments on initial report of the Privacy & Proxy (P&P) Accreditation PDP WG
IP WHOIS – Work with Numbering Resource Organisation (NRO) to help improve IP Address WHOIS accuracy	PSWG	Ongoing – PSWG meeting in Jan 2016 and at ICANN 55.	Public safety agencies, regional Internet registries and their members.	Report.
WHOIS case studies in several areas, including fee fraud investment scams and both	PSWG	Ongoing	Public safety agencies	WHOIS case studies compilation.

DNS WHOIS and IP WHOIS data.				
Next Generation Registration Directory Services (RDS)	PSWG members	August 2015, Ongoing	Public safety agencies	GAC comments on Next Generation Registration Directory Services, August 2015 Further contributions to the PDP.
3. CYBERSECURITY, CONSUMER PROTECTION				
Registry Agreement (RA): New gTLD "Spec 11" Security Framework	PSWG	Ongoing – ICANN Marrakesh	Public safety agencies	PSWG document presented to ICANN Security Framework Working Group (October 2015). PSWG input on security framework draft(s).
Registrar Accreditation Agreement (RAA): Addendum for Illegal/Counterfeit Drug Reporting to ICANN Contract Compliance	PSWG	Ongoing	Public safety agencies	Addendum draft.
New gTLD Competition, Consumer Choice and Consumer Trust Review mandated by the AoC	PSWG	Ongoing	Public safety agencies	To be confirmed.
Sensitive strings in new gTLDs	PSWG	Ongoing	Public safety agencies, child protection bodies	To be confirmed.

Legend: ▢ (green) Completed   ▢ Current, future or ongoing

Registrar Accreditation Agreement (RAA)

INTERNET GOVERNANCE

Link to 2013 RAA:
https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

What is the Registrar Accreditation Agreement?

The Registrar Accreditation Agreement (RAA) is the contract that governs the relationship between ICANN and its accredited registrars.

The RAA was originally one of several agreements between ICANN, the United States Department of Commerce (DOC), and Network Solutions, with the intent of enhancing and solidifying the competition between .com, .net, and .org TLD registrars. These agreements were tentatively announced on September 28, 1999, and, after oral and written public comments, were revised and then adopted by ICANN on November 4, 1999. At the time, registrars were allowed to take up the new agreement in place of their old agreement.

On May 21, 2009, ICANN approved revisions to the RAA, which were intended to clarify the responsibilities of the registrars and the rights of the registrants. These revisions came about in response to market development and the significant growth in the number of accredited registrars and domain name registrations, and through a comprehensive review of the RAA and the Accreditation process called for in March 2007 by then-ICANN CEO Paul Twomey. This new RAA applies to all the new registrars, registrars that voluntarily adopt the contract prior the renewal date, and to registrars that renew after the approval date. But, following this revision, there were still those who thought the RAA did not do enough to address public concerns. Thus the RAA Drafting Team was formed, made up of members of the GNSO and the At-Large Community, to propose further revisions.

Law enforcement officials, particularly the Serious Organized Crime Agency (SOCA) in the United Kingdom and the United States Federal Bureau of Investigation (FBI), asked ICANN to implement procedures to curb incidence of abuse in the domain name system (DNS). The two agencies proposed some measures to be incorporated in the RAA such as stronger verification of registrants' name, address, phone number, e-mail address and method of payment for domain names.

In October, 2011, at the ICANN 42 meeting in Dakar, Senegal, the ICANN Board approved the immediate negotiation between ICANN and Registrar Negotiation Team regarding the proposed amendments to the RAA. The amendment topics, which included law enforcement, registrant protection and internet stability, were recommended by the Governmental Advisory Committee (GAC) and the GNSO Working Group. The result of the amendment

negotiations were to be considered by ICANN during its meeting in Costa Rica in March, 2012.

The RAA Negotiation Team and ICANN indicated they had nearly reached agreement on a majority of the topics discussed during the 13 negotiation sessions, in both principles and language. You can find the Summary of RAA Negotiations here.

Development

In September, 2012, a working group related to the European Commission sent a letter to ICANN warning that its proposed additions to the RAA would infringe on European Privacy laws. The issues in question are the proposals to make registrars retain data about their customers for up to two years after registration, and by the idea that registrars should re-verify contact data every year. These proposals were discussed and supported by the GAC and the law enforcement voices within ICANN at ICANN 44 in Prague. This is potentially conflicting given that the GAC supported these measures and this pan-European body is coming down against it.

In October, 2012, just before the ICANN 45 Meeting in Toronto, ICANN CEO Fadi Chehadé stated that due to European privacy laws, European registrars may be exempt from the proposed new Whois verification requirements. It was emphasized that the GAC had already endorsed the measures, with relevant laws in mind. This suggestion would seemingly create 2 different RAAs, which would arguably create inequitable standards between international registrars. This came after another European body, the Council of Europe, expressed its concern over the privacy requirements in the proposed RAA.

In early 2013, ICANN and the Registrar Stakeholder Group hit an impasse in their negotiations. It seems that while they agree on many points, with both sides making concessions and compromises, the main sticking point was ICANN's insistence on a unilateral right to amend, which was also a contentious addition to ICANN's new Registry Agreement for new gTLD operators. The addition would give the ICANN Board the right to amend the RAA in any way it sees fit by a 2/3 majority vote. It seems that this may be part of new CEO, Fadi Chehadé's, strategy at making the industry more accountable and better regarded, and also a way to avoid extended debate and negotiations over future contracts. ICANN published its suggested agreement for public comments in the midst of ongoing negotiations, given that the efforts had stalled.

Points of agreement include: new Whois accuracy measures, featuring a challenge-response mechanism for first-time registrants via email or phone verification; addresses submitted will have to meet the Universal Postal Union

standards, and phone numbers must conform to ITU formatting; the address will have to be verified to be an actual location, though proof of residence or ownership by the registrant will not be required; registrants providing false information that fail verification will have 15 days to correct the information before facing suspension of the domains. A further sticking point beyond the unilateral right to amend is ICANN's request that registrars verify their customer records, which tend to be more accurate than Whois records.

During ICANN 46 in April of 2013, newer versions of the RAA and the Registry Agreement were both published for public comment. After weeks of negotiations and drafts, the new RAA was approved by the ICANN board on June 27, 2013. It applies for all Registrar Accreditation Agreements entered into after 28 June 2013, regardless of whether for new or old (e.g. .org, .biz) gTLD. Only registrars on the 2013 RAA are permitted to sell registrations in new gTLDs.

For more information, please see here:
https://www.icann.org/resources/pages/registrars/registrars-en.

Source: ICANNwiki RAA: http://icannwiki.com/RAA

Highlights of 2013 RAA

The 12 Law Enforcement Recommendations that served as the impetus for these negotiations are all addressed in the 2013 RAA. The Law Enforcement Summary Chart below identifies the section or specification of the 2013 RAA that addresses each recommendation. This includes the creation of an abuse point of contact at each registrar, Whois verification and validation requirements at the registrant and the account holder levels, stronger registrar obligations for resellers, and new data retention obligations for registrars.

Highlights include:

- A detailed **Whois accuracy program specification** outlining registrars' obligations to verify and validate key data provided by registrants within 15 days of registration, including email address and phone number. In the absence of cooperation by the registrant in the verification process, the registrar shall terminate or suspend the agreement giving use of a domain name to the registrant.
- **Enhanced compliance tools** including broader suspension and termination tools, clarification of audit rights and access to information to facilitate ongoing investigations, and annual certification requirements.
- **Registrar responsibility** for reseller compliance with all appropriate terms of the RAA.
- **Consolidation with the Registry Agreement for new gTLDs**. Where appropriate, language from the Registry Agreement is mirrored to allow for contracts that are better aligned. The new gTLD Registry Agreement and the 2013 RAA should complement each other.
- **Proxy and Privacy Provider Interim Requirements**.[2] Until a formal accreditation program is developed, interim protections are put in place for proxy and privacy services offered through registrars. These interim protections will require that information is made available on items such as customer service processes and when a provider will relay information on the underlying user of the domain name registration.

Annexed to the 2013 RAA, ICANN also adopted a **Registrant Rights and Responsibilities Document** that sets out, in clear and simple language, the rights and responsibilities of the registrant under the 2013 RAA, such as the types of information that should be made available to registrants about terms and conditions of registrations, fees and customer service processes. The document also emphasizes the registrant's role in providing accurate contact information, and responsibilities in maintaining domain name registrations.

---

[2] See p. 47 below for more information on proxy and privacy services.

How the 2013 RAA Addresses Law Enforcement Recommendations
22 April 2013

	Summary of LE Recommendation	**RAA Reference**
1	Registrar duty to investigate reports of illegal conduct, including responding to reports from law enforcement, and providing a system to track complaints	• Section 3.18, requiring Registrars to maintain an abuse point of contact and provide a trackable system
2	Registrar shall not engage in activities or conduct that results in: (i) a conviction by a court of competent jurisdiction of a felony or other serious offense related to financial activities; (ii) a judgment by a court of competent jurisdiction that Registrar has committed fraud or breach of fiduciary duty; (iii) the Registrar being the subject of a judicial determination that is the substantive equivalent of those offenses (i)-(ii); or (iv) the Registrar knowingly and/or through gross negligence, permitting criminal activity in the registration of domain WHOIS information, after failing to promptly cure such activity after notice thereof.	• Section 5.5, which includes heightened and additional termination remedies
3	Registrar collection of data regarding registrations in addition to the data already collected.	• The Data Retention Specification includes new items of data for retention and maintenance
4	Registrars abuse contact – posting of contact information and having a contact available around the clock	• Section 3.18, requiring Registrars to maintain an abuse point of contact
5	Publication of registrar information, including contact details, as well as regular updates to ICANN regarding changes in registrar business information	Section 3.17.1 will now require registrars to provide updates to ICANN of the type of information that is required upon application for accreditation
6	Disclosure of affiliated registrars and affiliated businesses	Section 3.17.1 (see item 5) incorporates this disclosure

7	Privacy and Proxy Services – Escrow, Reveal and Relay	• Section 3.14, regarding the development of an ICANN accreditation program • Proxy/Privacy Specification, putting in place interim requirements for proxy/privacy services offered through registrars
8	ICANN Accreditation of Proxy and Privacy Services	• See item 7.
9	Accountability of Resellers – Resellers must be held completed accountable to all provisions of the RAA.	• Section 3.12, imposing heightened obligations in relation to resellers
10	Registrar validation of registrant data	• Whois Accuracy Specification, setting out requirements for validation and verification of registrant and account-holder data
11	Whois service level agreements, with uptime minimums and specifying data update requirements	• Whois SLA now includes these requirements
12	Expansion of grounds of termination of RAA for criminal convictions, including "knowingly and/or through gross negligence permit criminal activity in the registration of domain names or provision of domain name WHOIS information…"	• Section 5.5, which includes heightened and additional termination remedies

Specification 11 Security Framework for Registry Agreement

INTERNET GOVERNANCE

Specification 11 Security Framework Overview

In its 2013 Beijing Communiqué (reproduced below), the GAC called upon ICANN to oblige new gTLD registries to perform a certain amount of abuse mitigation and security checks. These obligations were translated into a separate part of the new gTLD Registry Agreement, the so-called Specification 11 (or "Spec 11" for short), which contains all commitments the registries undertake in the public interest. The Spec 11 is also reproduced below. As the obligations in the Spec 11 are fairly high-level, a process is ongoing to identify examples of best practice and, on that basis, to develop a nonbinding framework for registries to ensure that sites under their TLD are not being abused or used to create security threats. A first comprehensive draft framework is expected to be released for public comment in early 2016.

The following infographic provides an overview of the ongoing process for the development of the framework:

Project: Spec 11 Security Framework

Define implementation details of the Security checks called for by the NGPC's Proposal for Implementation of GAC Safeguards Applicable to All New gTLD (Resolution 2013.06.25.NG02). Develop a Framework for Registry Operators to conduct periodic security checks and respond to identified security threats in consultation with the community.

Planned Start Date: 2014-08-20

Planned Completion Date: 2016-08-01

Metrics: Release of security framework including Safeharbor provisions for RA Spec 11 3b

Dependencies: Staff, Community Engagement: Registry GAC Public Comments

Stakeholders: SSR, Registry, Registrar, GAC, Legal, Contractual Compliance

Topics: Security, Abuse, Registry, Registrar, GAC, Registry Agreement, Contractual Compliance

Last Updated: December 1, 2015 - 02:51

Project Status

On Target
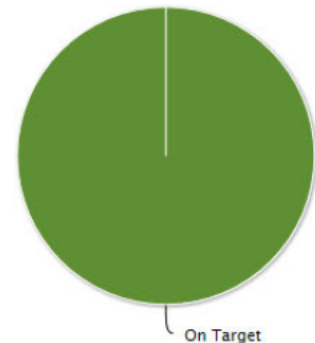
Beijing Communiqué Annex 1 – Safeguards on New gTLDs

The GAC considers that Safeguards should apply to broad categories of strings. For clarity, this means any application for a relevant string in the current or future rounds, in all languages applied for.

The GAC advises the Board that all safeguards highlighted in this document as well as any other safeguard requested by the ICANN Board and/or implemented by the new gTLD registry and registrars should:

- Be implemented in a manner that is fully respectful of human rights and fundamental freedoms as enshrined in international and, as appropriate, regional declarations, conventions, treaties and other legal instruments – including, but not limited to, the UN Universal Declaration of Human Rights.
- Respect all substantive and procedural laws under the applicable jurisdictions
- Be operated in an open manner consistent with general principles of openness and non-discrimination.

Safeguards Applicable to all New gTLDs

The GAC advises that the following six safeguards should apply to all new gTLDs and be subject to contractual oversight.

- **WHOIS verification and checks** – Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberatively false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberatively false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.

- **Mitigating abusive activity** – Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

- **Security checks** – While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies

security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.

- **Documentation –** Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.

- **Making and Handling Complaints -** Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

- **Consequences –** Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirements that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.

SPECIFICATION 11 of the Registry Agreement
PUBLIC INTEREST COMMITMENTS

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on 27 June 2013 in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.

2. Registry Operator will operate the registry for the TLD in compliance with all commitments, statements of intent and business plans stated in the following sections of Registry Operator's application to ICANN for the TLD, which commitments, statements of intent and business plans are hereby incorporated by reference into this Agreement. Registry Operator's obligations pursuant to this paragraph shall be enforceable by ICANN and through the Public Interest Commitment Dispute Resolution Process established by ICANN (posted at
http://www.icann.org/en/resources/registries/picdrp), which may be revised in immaterial respects by ICANN from time to time (the "PICDRP"). Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination

   [Registry Operator to insert specific application sections here, if applicable]

3. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

   a. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary

to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

c. Registry Operator will operate the TLD in a transparent manner consistent with general principles of openness and non-discrimination by establishing, publishing and adhering to clear registration policies.

d. Registry Operator of a "Generic String" TLD may not impose eligibility criteria for registering names in the TLD that limit registrations exclusively to a single person or entity and/or that person's or entity's "Affiliates" (as defined in Section 2.9(c) of the Registry Agreement). "Generic String" means a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others.

WHOIS

INTERNET GOVERNANCE

WHOIS Primer
(http://whois.icann.org/en/primer)

This WHOIS Primer summarizes the key components of the WHOIS service, policy, and protocols. It takes into account the many contracts, specifications, standards, protocols, advisories, and policies that collectively describe the ICANN WHOIS program applicable to the collection, display, and use of gTLD domain name registration data.

This Primer is based on the obligations described in the 2013 Registrar Accreditation Agreement (2013 RAA), and the base new gTLD Registry Agreement (New GTLD Registry Agreement) and in a few instances other registry agreements, as noted below. As not all registrars and registries are operating under the 2013 RAA or the New gTLD Base Agreement, their actual obligations pertaining to WHOIS may vary. Please refer to the language of the original documents for the text of the obligations related to WHOIS.

1. Introduction to WHOIS
2. Uses of WHOIS
3. WHOIS Requirements
4. WHOIS in Domain Name Management and Dispute Resolution Procedures
5. Updating or Modifying ICANN'S WHOIS Program
6. Disclaimer

1. Introduction to WHOIS

The Affirmation of Commitments requires ICANN to "implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information…" The WHOIS service is a free, publicly available directory containing the contact and technical information of registered domain name holders (referred to as "registrants"). Anyone who needs to know who is behind a website domain name can make a request for that information via WHOIS. The data is collected and made available by registrars and registries under the terms of their agreements with ICANN.

WHOIS is not a single, centrally managed database. Rather, registration data is held in disparate locations and administered by multiple registries and registrars. They set their own conventions for WHOIS service, consistent with the minimum requirements established in their ICANN contracts.

The term "WHOIS" refers to protocols, services, and data types associated with Internet naming and numbering resources beyond domain names, such as Internet Protocol (IP) addresses, and Autonomous System Numbers (ASNs). The WHOIS service includes WHOIS clients, WHOIS servers, WHOIS data stores, and

WHOIS data (domain name registration records). Essentially, WHOIS can refer to any of the following:

1. The information that is collected at the time of registration of a domain name or IP numbering resource and subsequently made available via the WHOIS Service, and potentially updated throughout the life of the resource;

2. The WHOIS Protocol itself, which is defined in RFC 3912; or

3. The WHOIS Services that provide public access to domain name registration information typically via applications that implement the WHOIS protocol or a web-based interface.

These ambiguities inherent in the WHOIS label complicate efforts to shape the evolution of meta-data for Internet naming and numbering. To address this, ICANN has developed more precise terminology for gTLDs, including:

Domain Name Registration Data (DNRD) – refers to the information that registrants provide when registering a domain name and that registrars or registries collect. Some of this information is made available to the public. For interactions between ICANN accredited Generic Top Level Domain (gTLD) registrars and registrants, the data elements are specified in the current registry agreement and Registrar Accreditation Agreement. For country code Top Level Domains (ccTLDs), the operators of these TLDs implement local policy regarding the request and display of registration information.

Domain Name Registration Data Access Protocol (DNRD-AP) – refers to the elements of a (standard) communications exchange—queries and responses— that make access to registration data possible. For example, the WHOIS protocol (RFC 3912) and Hypertext Transfer Protocol (HTTP) (RFC 2616 and its updates) are commonly used to provide public access [PDF, 649 KB] to DNRD.

Domain Name Registration Data Directory Service (DNRD-DS) – refers to the service(s) offered by registries and registrars to provide access to (potentially a subset of) the DNRD.

2. Uses of WHOIS
Internet operators use WHOIS to identify individuals or entities responsible for the operation of a network resource on the Internet. Over time, WHOIS has evolved to serve the need of many different stakeholders, such as registrants, law enforcement agents, intellectual property and trademark owners, businesses and individuals.

Stakeholders use the WHOIS service for a variety of purposes, including to:

- Determine whether a domain is available
- Contact network administrators regarding technical matters
- Diagnose registration difficulties
- Contact web administrators for resolution of technical matters associated with a domain name
- Obtain the real world identity, business location and contact information of an online merchant or business, or generally, any organization that has an online presence
- Associate a company, organization, or individual with a domain name, and to identify the party that is operating a web or other publicly accessible service using a domain name, for commercial or other purposes
- Contact a domain name registrant for the purpose of discussing and negotiating a secondary market transaction related to a registered domain name
- Notify a domain name registrant of the registrant's obligation to maintain accurate registration information
- Contact a domain name registrant on matters related to the protection and enforcement of intellectual property rights
- Establish or look into an identity in cyberspace, and as part of an incident response following an Internet or computer attack- (Security professionals and law enforcement agents use WHOIS to identify points of contact for a domain name)
- Gather investigative leads (i.e., to identify parties from whom additional information might be obtained)- Law enforcement agents use WHOIS to find email addresses and attempt to identify the location of an alleged perpetrator of a crime involving fraud
- Investigate spam- law enforcement agents look to the WHOIS database to collect information on the website advertised in the spam

Under the ICANN contracts, WHOIS can be used for any legal purpose except to enable mass unsolicited, commercial advertising or solicitations, or to enable high volume, automated, electronic processes that send queries or data to a registry or registrar's systems, except as necessary to manage domain names.

3. WHOIS Requirements
Anyone wishing to register a domain name must provide contact and technical information for display in the WHOIS database; WHOIS data is actually a subset of the information due at the time of registration.

In turn, ICANN's agreements with registrars require them to provide public access to data on registered names. The 2013 RAA states that "at its expense,

Registrar shall provide an interactive web page and, with respect to any gTLD operating a "thin" registry, a port 43 WHOIS service (each accessible via both IPv4 and IPv6) providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar in any gTLD."

For the generic top-level domain (gTLD) registries, ICANN specifies WHOIS service requirements through the registry agreements. Registries satisfy their WHOIS obligations using different services. The two common models are often characterized as "thin" and "thick" WHOIS registries. Although all new gTLD registries operate a thick registry, currently a few existing registries (such as .COM and .NET) operate a thin registry. A thin registry only includes data sufficient to identify the sponsoring registrar, status of the registration, creation and expiration dates for each registration, name server data, and last time the record is updated in its WHOIS data store. Thick registries maintain the registrant's contact information and designated administrative and technical contact information, in addition to the sponsoring registrar and registration status information supplied by a thin registry.

Additionally, registrants are required to provide timely updates (within seven days) to WHOIS data for a registered domain name. The registrar is then obligated to promptly update the WHOIS data.

Accuracy
Because registration data connects individuals or organizations with domain names, registrants are required to provide accurate and reliable contact details. If the registrant knowingly provides inaccurate information, fails to update information within seven days of any change, or does not respond within 15 days to an inquiry about accuracy, the domain name may be suspended or cancelled.

For their part, registrars are required to comply with the new WHOIS Accuracy Specification. They must verify certain WHOIS fields such as email addresses or phone numbers and validate the presence of data as well as the format of email addresses, postal addresses and telephone numbers. Registrars are also obliged to send annual data reminder notices to registrants and to verify and validate changes to WHOIS data.

Registrars are obligated to perform these validation and verifications of these WHOIS data fields within fifteen days of the domain registration, inter-registrar transfer, or any change in the registrant.

However, if a Registrar has already successfully completed the validation and verification procedures on the identical contact information, and is not in

possession of facts or knowledge of circumstances that suggest that the information is no longer valid, then it is not obligated to re-validate or re-verify these WHOIS data fields.

Anyone can submit complaints of inaccuracies through ICANN's WHOIS data reporting system, and the RAA requires registrars to investigate claims of inaccuracy. Registrars must also re-verify and re-validate certain WHOIS data fields if they have any information suggesting that these WHOIS data fields are incorrect.

In order to verify and ensure the operational stability of registry services, as well as to facilitate compliance checks on accredited registrars, registry provide ICANN with weekly, specific up-to-date thin registration data. Registries also are required in exceptional cases, such as failure of a registry, to provide bulk access to thick registration data to ICANN.

Access
Registrars and registries [PDF, 649 KB] are obligated to provide access to WHOIS data through registration data publication services. It must be publicly available in a specific format and on a designated "port" reserved for WHOIS data sharing (port 43), as well as on an interactive webpage. Port 43 access by registrars is required only for domain names registered in 'thin' registries. The data must include specific identification, contact and technical information.

At present, web-based WHOIS queries may be performed through the websites of ICANN accredited registrars and registries, most regional Internet registries, and third party WHOIS client providers. The agreement between a gTLD registry operator and registrar may, if approved by ICANN in writing, state alternative requirements for that gTLD. Also, under certain market conditions, the registrar may be obligated to provide bulk access to WHOIS.

Data available depends on whether a registry is "thick" or "thin". Only a few registries that existed prior to the new GTLD program are "thin," (such as .com and .net). Thin registries do not include registrant contact details. For thin registries, registrars provide the specific registrant contact information.

ICANN specifies Service Level Agreements related to the performance and acceptable downtime of the registrar & registry's WHOIS services. This includes downtime for maintenance, planned outages or system failures, and performance response times to Internet user queries.

Anyone can submit a complaint that a registrar's WHOIS service is down. Registries must submit WHOIS performance reports to ICANN.

Reseller Related Obligations
To the extent that a reseller is involved in facilitating a registration of a domain name, registrars are obligated to comply with all WHOIS obligations.

Obligations of Licensors of Domain Names
Licensors of domain names also have responsibility for the actions of licensees. Any registrant that licenses use of a domain name to a third party is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A registrant licensing use of a domain name is liable for harm caused by wrongful use of the domain name, unless it discloses the current contact information provided by the licensee and the identity of the licensee within seven (7) days to a party providing the registrant reasonable evidence of actionable harm.

Data Escrow
ICANN requires registrars to submit an electronic copy of the registrar's database, which includes WHOIS data, to a reputable escrow agent on a schedule, under the terms, and in the format specified by ICANN.

Registries are required [PDF, 649 KB] to deposit domain name registration data, along with other registry data, in escrow, with an escrow agent.

Centralized WHOIS
The RAA specifies that if the WHOIS service implemented by registrars does not provide reliable and convenient access to accurate and up-to-date data, ICANN may set up a centralized database.

In response to the WHOIS Review Team's recommendations, ICANN has committed to creating a centralized look-up tool that will interface with the WHOIS databases of registrars and registries to simplify and make the WHOIS service more convenient for its users.

Data Elements
The format of responses must contain certain data elements and follow a semi-free text format. A list of the available data elements and directions about which ones are required/mandatory is included in the Registration Data Directory Services Specification to the 2013 RAA.

There are also specific formatting requirements for registrars and registries.

Internationalized Registration Data

At the moment, the current specifications do not include language or script requirements for input or output. Work is underway to internationalize WHOIS, and placeholders are included in the 2013 RAA and Registry Agreement to incorporate for future rules being developed by IETF or the ICANN community.

Searchability Features
Registries have the option to provide certain search functionality for the WHOIS.

Privacy Considerations
Registrars must notify each new or renewed Registered Name Holder as to the purpose of the personal data collected. The registrant must also consent to the data processing.

Registrars and registries must comply with applicable laws and government regulations regarding the collection, display and distribution of personal data via WHOIS. If a registrar or registry encounters a conflict with local laws, ICANN has procedures in place for reviewing and considering those situations.

Privacy/ Proxy Services
Privacy and proxy services are for individuals and entities who wish to keep certain information from being made public via WHOIS.

There are two general types of these services:

- A *Privacy Service* lists alternative, reliable contact information, like an address or phone number, in WHOIS while keeping the domain name registered to its beneficial user as the registrant.
- A *Proxy Service* registers the domain name itself and licenses use of the domain name to its customer. The contact information of the service provider is displayed rather than the customer's contact information. The proxy service is responsible for providing accurate contact information adequate to facilitate timely resolution of any problems that arise in connection with the domain name. The proxy service accepts liability for harm caused by wrongful use of the name unless it promptly discloses the identity of the licensee to a party providing reasonable evidence of actionable harm.

Privacy and Proxy Services offered by Registrars or their affiliates are subject to additional obligations. These Privacy and Proxy Providers must disclose their Service Terms, publish an Abuse of Point Contact and meet Escrow Obligations.

Educating Registrants about WHOIS
Registrars and Registries [PDF, 649 KB] must provide Registrants certain WHOIS policy and educational information.

Benefits and Responsibilities Documents

Every registrar must publish on its website(s) and/or provide a link to the Registrants' Benefits and Responsibilities Specification.

Registrants' rights include:

Instructions that explain the registrar's processes for registering, managing, transferring, renewing, and restoring domain name registrations, including through any proxy or privacy services made available by the Registrar.

Registrants' Responsibilities include:

Providing accurate information for publication in directories such as WHOIS, and promptly update the data to reflect any changes.

4. WHOIS in Domain Name Management and Dispute Resolution Procedures

WHOIS is referenced to conduct specific functions related to the operation of domain names. For example, WHOIS is used to support the transfer or deletion of a domain name, or to facilitate trademark related administrative dispute resolution proceedings such as the Uniform Dispute Resolution Policy (UDRP) and the Uniform Rapid Suspension System (URS).

Transfers

Under the ICANN Policy on Transfers Between Registrars, the authority to transfer a domain name is restricted to the administrative contact and the registered name holder in the WHOIS record. The gaining registrar must obtain a valid Form of Authorization (FOA) from either of these contacts.

If the transfer between registrars is contentious, the Registrar Transfer Dispute Policy allows a registry to examine the WHOIS evidence to determine if the transfer was properly authorized.

Deletions

Sometimes registrations are deleted – such as in the case of false contact data or a non-response to registrar inquiries. Under the Expired Domain Name Recovery Policy, the Registrant at Expiration in the WHOIS record is offered a Redemption Grace Period of 30 days to request the restoration of a domain name. During this time, the registered domain name is disabled and cannot be transferred.

Under the Restored Names Accuracy Policy, following the restoration of the domain name, the domain name registration must be placed on hold until updated and accurate WHOIS information is provided.

Uniform Dispute Resolution Policy (UDRP)

Under the rules for the UDRP, the WHOIS record is referenced to:

- Identify the Registrant to be named in a UDRP Complaint as the respondent.
- Determine appropriate jurisdiction for any court proceedings related to a UDRP case.
- Determine whether the registrar has properly "locked" the registration. Once a UDRP complaint is received, the registrar must "lock" the registration to prevent any transfers as long as the complaint proceeding is pending.

New gTLD Uniform Rapid Suspension System (URS)

WHOIS is also referenced in trademark related complaints in new gTLDs under the **Uniform Rapid Suspension** System (URS) to:

- Identify the Registrant to be named in a URS Complaint as the respondent.
- Confirm URS Locking: upon initiation of a complaint, a Notice of Complaint is sent by the Provider to the addresses listed in the WHOIS contact information that provides an electronic copy of the Complaint, advises of the locked status, as well as the potential effects if the Registrant fails to respond and defend against the Complaint.
- Notice of Default: If there is a default decision, a notice of default is sent to the addresses listed in the WHOIS.
- Confirm a URS suspension: the WHOIS record is updated to reflect that the domain name may not be transferred, deleted or modified.

5. Updating or Modifying ICANN'S WHOIS Program

Changes to WHOIS can occur in a variety of ways. The Affirmation of Commitments creates three-year review cycles, and those reviews can lead to modifications of WHOIS Policy. Changes to WHOIS obligations can also be accomplished through the contract amendment clauses in the RAA and in each of the Registry Agreements. In addition, consensus policies created through recommendations developed by the Generic Names Supporting Organization (GNSO) as approved by the Board in accordance with the procedures under the ICANN Bylaws, can also change WHOIS obligations

6. Development of a new Registration Directory Service (RDS) to replace WHOIS

A Policy Development Process (PDP) has been underway since 2012 to define the purpose of collecting, maintaining and providing access to gTLD registration data, to identify safeguards for protecting that data, and to improve the accuracy of WHOIS information. It also seeks to provide information to support a

decision on if and why a next-generation Registration Directory Service (RDS) is needed to replace WHOIS.

The PDP has encompassed a number of steps in the past, of which three notable ones are

1. the work of the WHOIS Review Team and its Final Report published in 2012, which led to the launch of the PDP (https://www.icann.org/en/system/files/files/final-report-11may12-en.pdf);
2. the work of the Expert Working Group on WHOIS and its Final Report published in 2014 (https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf);
3. and the Final Issue Report on new RDS, which seeks to further define the scope of an issue requiring policy development and set out the central issues relevant to the policy development (http://whois.icann.org/sites/default/files/files/final-issue-report-next-generation-rds-07oct15-en.pdf).

A full overview of the PDP can be found here: http://gnso.icann.org/en/group-activities/active/rds.

The most recent step in the PDP was the November 2015 resolution of the GNSO to officially initiate the PDP by endorsing the creation of a PDP Working Group, with a call for interest to be published no later than January 4, 2016.

GNSO Resolution: Approval of a charter for the Next-Generation gTLD Registration Directory Service (RDS) to replace WHOIS (Next-Gen RDS) PDP WG

1. Following submission of the WHOIS Policy Review Team's Final Report, the ICANN Board passed a resolution on 8 November, 2012, launching an Expert Working Group on gTLD Registration Directory Services (EWG) to (1) help redefine the purpose of gTLD registration data and consider how to safeguard the data, and (2) propose a model for gTLD registration directory services to address accuracy, privacy, and access issues.

2. Upon publication of the EWG's Final Report in June, 2014, an informal group of Generic Names Supporting Organization (GNSO) Councilors and ICANN Board members collaborated to propose a Process Framework for structuring a GNSO Policy Development Process (PDP) to successfully address these challenging issues.

3. On 26 May, 2015, the ICANN Board adopted that Process Framework and reaffirmed its 2012 request for a Board-initiated PDP to define the purpose of collecting, maintaining and providing access to gTLD registration data, and to consider safeguards for protecting data, using the recommendations in the EWG's Final Report as an input to, and, if appropriate, as the foundation for a new gTLD policy.

4. In accordance with the PDP Rules, a new Preliminary Issue Report was published for public comment on 13 July 2015. Following review of the public comments received, the Staff Manager updated the Issue Report accordingly and included a summary of the comments received (see Annex D), which was submitted as the Final Issue Report to the GNSO Council for its consideration on 7 October 2015.

5. The GNSO Council has reviewed the issues raised in the Final Issue Report as well as the Draft Charter for a PDP Working Group that was included in the Preliminary Issue Report and updated reflecting the input received in the Final Issue Report under Annex C (pp.67-77)

RESOLVED,

1. The GNSO Council approves the Draft Charter proposed in the Final Issue Report and appoints Susan Kawaguchi as the GNSO Council liaison to the Next-Generation gTLD Registration Directory Service (RDS) to replace WHOIS (Next-Gen RDS) PDP WG;

2. The GNSO Council directs ICANN staff to issue a call for volunteers for the PDP WG after the approval of this motion. The call for volunteers should be circulated as widely as possible in order to ensure broad representation and participation in the Working Group and should be initiated no later than January 4th, 2016 and remain open until the Working Group convenes for the first time; and

3. The Working Group (WG), when convened, is instructed to reach out to all Stakeholder Groups/Constituencies (SG/C) for additional feedback on any items that they believe should be considered that may not have been specifically called out in the charter. The WG is also expected to consider input already provided by SG/Cs during the public comment period on the Preliminary Issue Report. Should the WG be of the view that after the review of this feedback changes need to be made to the charter to address these, the WG is expected to come back to the Council with proposed changes to the charter for the Council to consider.

4. Until such time as the WG selects a chair(s) for the WG and that chair(s) is confirmed by the GNSO Council, the GNSO Council liaison to the WG shall serve as the interim chair.

Source: http://gnso.icann.org/en/council/resolutions#201511

.

Implementation Report on the WHOIS Improvements

Implementation Status of the *Board Approved*[1] WHOIS Review Team Final Report Recommendations As of 2 April 2015		**Key:** Complete √ or 🟢 In Progress ○ or 🔵 In Planning ◊ or 🟣	
	Topic	**Summary of Implementation Activities**	**Milestones & Due Dates[2]**
	WHOIS - Strategic Priority		
1.a 🟢	WHOIS as a strategic priority	WHOIS emphasized in Strategic Plan as part of Strategic Objective 2.1 and funded in the FY15 Operating Plan and Budget. WHOIS Program supervised by Strategic Initiatives Team and implemented through a cross-departmental effort. CEO oversaw improvements to WHOIS obligations in contracts, including: • Adoption of new 2013 Registrar Accreditation Agreement, which includes many Compliance and WHOIS related enhancements; • Adoption of New gTLD Registry Agreement requiring registrars to use 2013 RAA and incorporate many WHOIS improvements; and • Transition of 2013 RAA into existing registry agreements via renewals of registry agreements.	√ Final 5 Year Strategic Plan approved by ICANN Board – 16 Oct 2014. √ Allen Grogan appointed as the new ICANN Chief Contract Compliance Officer to oversee Contract Compliance and Consumer Safeguards enhancements, including WHOIS. – 10 Oct 2014. √ Registrars signed new 2013 RAA (2013 - 2018); List of Registrars on the 2013 RAA available here. √ New gTLD Registries now sign new registry agreements. List of registries available here. √ WHOIS Accuracy Specification of 2013 RAA to be reviewed annually. √ First review scheduled Early 2015 √ ICANN plans to solicit community feedback beginning in January 2015 and met with registrars in Singapore in 2015.
1.b 🟢	ICANN Staff incentivization	WHOIS projects identified in both AtTask and the Halogen management system. CEO compensation based on the overall goals and objectives of the entire organization set forth in AtTask.	
1.c 🟢	Board involvement in WHOIS improvements	Board updated, on a trimester basis on the status of WHOIS related activities and implementation.	

1.d 🟢	Public Status of Implementation	Public closely apprised of the implementation progress through regular updates, announcements on icann.org, blog posts, updates at ICANN meetings, the new WHOIS website, and webinars.	√ ICANN Blog on the Debut of the Beta Launch of the WHOIS Website – Phase I – 4 Nov 2013
			√ ICANN Buenos Aires Sessions:
			  √ Contractual Compliance Program Update – 20 Nov 2013
			  √ Improving WHOIS, an Update – 21 Nov 2013
			√ ICANN Singapore Sessions:
			  √ Contractual Compliance Program Updates and Q&A Session – 26 Mar 2014
			√ ICANN London Sessions:
			  √ GAC Meeting: ICANN Overview on WHOIS – 22

[1] This Summary highlights ICANN's progress in 2014 measured against the Action Plan approved by the ICANN Board in its 8 November 2012 meeting. In some instances, the Action Plan adopts an alternative approach to implementing the recommendations from those proposed in the WHOIS Policy Review Team Final Report.

[2] See Appendix A of the WHOIS Improvements 2013 Annual Report for previously completed Milestone and Due Dates.

			June 2014 √ Contractual Compliance Program Updates and Q&A Session – 25 June 2014 √ ICANN Board Response to GAC London Communiqué – 3 Nov 2014 √ ICANN Los Angeles Sessions: 　√ GAC Meeting: WHOIS – 12 Oct 2014 　√ All Things WHOIS - Now and in the Future – 13 Oct 2014 　√ ICANN Board Response to GAC Los Angeles Communiqué –22 Jan 2015 √ ICANN Singapore Sessions: 　√ All Things WHOIS – 9 Feb 2015 　√ GAC Meeting: WHOIS – 10 Feb 2015 √ Status of Improvements published on new WHOIS Website √ ICANN Blog on WHOIS Primer and Global Look-Up Tool – 24 Jan 2014 √ ICANN Blog on a Model for Exploring WHOIS Accuracy – 3 Mar 2014 √ Draft Implementation Plan for the WHOIS Online Accuracy and Reporting System published – 11 Mar 2014 √ Public Comment Forum on Draft Implementation Plan for WHOIS Online Accuracy Reporting System – 11 Mar 2014 　√ Public Comment Forum on Draft Implementation Plan for WHOIS Online Accuracy Reporting System – 11 Mar 2014, closed 22 Apr 2014 　√ Staff Report published – 1 Mar 2014 √ ICANN Blog on Introducing the Beta Launch of the New ICANN WHOIS Lookup Tool – 9 Apr 2014 √ Announcement on Additional WHOIS Information Policy (AWIP) – 2 Jul 2014 √ Announcement on WHOIS Service Clarifications – 12 Sep 2014 √ ICANN Blog on What's Up with WHOIS – 10 Oct 2014 √ Series of webinars have been completed and are planned for future updates. √ ICANN's Quarterly Stakeholder Calls cover key operational developments, including WHOIS – Nov 2014 √ ICANN Blog on WHOIS: A Year in Review 15 Dec 2014 √ Initial Report from PDP Working Group on Translation and Transliteration of contact information published - 15 Dec 2014 　√ Public Comment on Initial Report from PDP Working Group on Translation and Transliteration of contact information – 16 Dec 2014, closed 1 Feb 2015 　√ Staff Report published - 19 Feb 2015 √ GNSO Translation and Transliteration of Contact Information PDP Webinar – 9 Jan 2015
2 🟢	**Single WHOIS Policy**	A Single Page containing links to all WHOIS related agreements and consensus policies developed.	√ Publication of an "easy to read" WHOIS Primer on the WHOIS microsite – 24 Jan 2014 √ Continued updates of the WHOIS Primer and the Knowledge Center
3	**Outreach:** ICANN should ensure that WHOIS policy	Requirements that link to Registrant Benefits & Responsibilities Document, written in simple language to educate registrants on obligations related	√ ICANN Blog on The 2013 Registrar Accreditation Agreement - What You Need to Know – 13 Feb 2014 √ ICANN Blog on the Update on 2013 RAA and Data

🟢	issues are accompanied by cross-community outreach	to WHOIS, included in the 2013 RAA.	Retention Waiver Process – 28 Feb 2014 √ ICANN Singapore Session on 2013 RAA FAQs – 26 Mar 2014
		ICANN Staff conducted global outreach to registrars to educate them on new 2013 RAA requirements.

ICANN Contractual Compliance Staff conducted outreach in Asia/Pacific, highlighting WHOIS obligations in native languages.

New WHOIS microsite launched:
  • Published in six languages; and
  • A one-stop-shop for those seeking information about WHOIS. | √ The 2013 RAA introduced improvements to WHOIS data with stricter validation and verification requirements. √Contractual Compliance updates regularly provided at the ICANN meetings.   The latest one was held in Singapore at ICANN 52 – Feb 2015

√ Completed system, FAQ, forms and Staff training to ensure 2013 RAA readiness. Please refer to this link for more details. √ Implementation of a Communications Plan to commence with the WHOIS Website launch √ Frequent updates through social media, such as twitter and Facebook in all UN languages. |
| 4 🟢 | **Contractual Compliance:** to managed in accordance with best practice principles | New Compliance complaints handling systems and procedures have been implemented.

Greater visibility on WHOIS-related metrics and improvements to Compliance processes and results has been achieved. | √ Launched WHOIS inaccuracy bulk complaints submission process and tool – 1 Nov 2013

√ Launched a WHOIS inaccuracy quality check on already resolved inaccuracy issues to confirm ongoing compliance √ Completed updates and additions to the complaint submission forms and FAQs for the 2013 RAA √ Compliance 2013 Annual Report published – Feb 2014, and 2014 Annual Report published – Feb 2015 √ Compliance Performance Reports now available |
| | | New 3 year Compliance Program on key registrar/registry obligations, including greater visibility on WHOIS-related metrics and improvements to Compliance processes and results | √ Launch a Three Year Audit Program (ending 2015):
  √ Completed Year 1 Audit published here
  √ Completed Year 2 Audit Program – May 2014
  √ 2013 Compliance Year Two Audit Report – July 2014 |
| | | New Registry Agreement Audit Program put in place. | √ Completed the plan and details for new Registry Agreement Audit program (New gTLD scope) √ Conducted 3 Audit outreach activities with registries. √ Updates to Audit page reflected new program and additional FAQ. Completed the first round of the new Registry Agreement Audit; link to the report: √ 2014 Contractual Compliance New Registry Agreement Audit Report 30 Jan 2014

√ Additional Compliance Department outreach activities. |
| | | Compliance Staffing levels increased substantially and resources were allocated for additional headcount. | √ Compliance Staff levels published and updated regularly. Current Staffing covers the following languages: Arabic, English, French, Korean, Mandarin, Russian, Spanish, Turkish, and Uzbek. √ Compliance established in 3 regions; Los Angeles, Istanbul and Singapore. |
| | **Data Accuracy** | | |
| 5 | WHOIS requirements for accurate data | Staff developed a WHOIS Informational Website to:
  • Provide historical record of WHOIS; | See answers to #3.

√ Public launch of WHOIS Informational Website – |

●		widely and pro-actively communicated	• Consolidate WHOIS policy documentation; • Provide mechanisms to teach people how to use WHOIS; • Provide mechanisms for people to submit complaints as they relate to WHOIS data; • Direct people to the appropriate channels to become engaged in the community on WHOIS related topics; • Educate registrants on WHOIS, their rights and responsibilities; and • Provide a Knowledge Center where key WHOIS related documents can be located.	4 Nov 2013 √ Public Launch of foreign translations of WHOIS Information Website – Nov 2013 √ Communications Plan kick-off for roll-out of WHOIS Informational Website – Nov 2013 √ Usage of the WHOIS microsite has grown since its launch to over 173,000 unique page views.
6	●	ICANN should take appropriate measures to reduce the number of WHOIS registrations that fall into the accuracy groups "Substantial Failure and Full Failure"	To address this recommendation, the Board directed the CEO to: • Proactively identify potentially inaccurate gTLD data registration information in gTLD registry and registrar services, explore using automated tools, and forward potentially inaccurate records to gTLD registrars for action; and • Publicly report on the resulting actions to encourage improved accuracy.	See answers to #7 & 11 below for information on the statistics on accuracy to be gathered in connection with the new WHOIS Search Portal.

7	●	Annual WHOIS accuracy reports	Staff is developing a WHOIS Accuracy Reporting System based on the methodology used by NORC at the University of Chicago.
			
			To accomplish the requested analysis, Staff's work is focusing on:
			
			• Statistical methodology;
			• Access to WHOIS records;
			• Parser to automate contact data extraction;
			• Automated address verification; and
			• Call center to call sampled records.
			
			Staff conducted a Pilot Accuracy Study in collaboration with NORC to test the proposed methodology using commercial validation services to test the syntactical and operation accuracy of the email, telephone number, and postal addresses using actual data of approximately 100,000 WHOIS records.
				√ Selected vendors and contracted for Draft Design of Experiment – Jan 2014.
				√ ICANN Blog on a Model for Exploring WHOIS Accuracy – 3 Mar 2014.
				√ Public Comment Forum on Draft Implementation Plan for WHOIS Online Accuracy Reporting System – 11 Mar 2014, closed 22 Apr 2014.
				
				√ Published Request for Proposal based on Final Implementation Plan for WHOIS Online Accuracy Reporting System – 19 May 2014.
				√ Completed contracting with selected vendors for WHOIS Online Accuracy Reporting System – Aug 2014.
				
				√ Published Pilot Study for the WHOIS Accuracy Reporting System: Preliminary Findings – 10 Oct 2014 with regular updates planned.
				  √ Community feedback on Pilot Study during ICANN 51 – Oct 2014.
				√ Publication of Final Pilot Study Report – 23 Dec 2014.
				  ○ Public Comment – 23 Dec 2014, closed 13 Mar 2015
				  ◊ Staff Report published – 3 Apr 2015
				
				◊ IAG to be formed to recommend the process for the follow-up procedure – Early 2015
				◊ IAG Process Recommendations published for Public Comment – TBD
				  ◊ Staff Report due – TBD
				◊ IAG Process finalized and launched - TBD
				
				◊ Modifications to Accuracy Reporting System –Apr – Jun 2015
				◊ Launch of Accuracy Reporting System - Phase I (Syntactic validation) – Aug 2015
				◊ Launch of Accuracy Reporting System - Phase II (Operational validation) – Late 2015
				◊ Launch of Accuracy Reporting System - Phase III (Identity validation, if at all) TBD

				√ Compliance Pilot planned to address potentially inaccurate records – Dec 2014 √ Initiated Compliance Pilot – Dec 2014 √ Review data & notify registrars of their volume – Feb 2015 ○ Begin enforcement of breaches
8		ICANN should ensure that there is a clear, unambiguous and enforceable chain of contractual agreements	Additional enforcement provisions and sanctions applicable to registrars, registrants, and resellers with regards to WHOIS included in 2013 RAA. Enhanced WHOIS obligations included in New gTLD Registry Agreements. Renewals of existing gTLDs includes enhanced WHOIS obligations. WHOIS Accuracy specifications of the 2013 RAA reviewed annually.	See answers to #1.a above.
9		**Compliance Metrics:** Impact of the annual WHOIS Data Reminder Policy (WDRP)	The Board's Resolution addressing the WHOIS Review Team Recommendations offers an alternative approach to achieving the intended result of this Recommendation.	See answers to #5 - 7 above.
10		**Data Access – Privacy and Proxy Services:** ICANN should initiate processes to regulate and oversee privacy and proxy service providers	New obligations related to Privacy/Proxy providers and commits ICANN to create a privacy/proxy accreditation program are included in the 2013 RAA. A GNSO PDP, beginning Oct 2013, has commenced to examine policy issues related to privacy/proxy services. A consensus policy, if produced out of the PDP, would become binding upon contracted parties when adopted by Board. Staff Implementation work to develop the operational aspects of the Privacy/Proxy Accreditation Program is to be conducted in parallel with GNSO PDP.	√ GNSO PDP on Privacy/Proxy Services commenced – Oct 2013 √ Charter for PDP on Privacy/Proxy Services approved by GNSO – 31 Oct 2013 ◊ PDP Initial Report release – estimated Apr 2015 ◊ PDP Final Report – estimated June 2015 ◊ GNSO approval of submitted IAG PDP Recommendation – estimated Aug 2015 ◊ Board Approval of PDP Recommendations – estimated July 2015 √ Staff presented a preliminary set of Privacy/Proxy Service Accreditation Program implementation alternatives to the Privacy Proxy Service Accreditation Issues Working Group for feedback – 10 Oct 2014
11		**Data Access – Common Interface:** Overhaul of the Internic Service	ICANN developed a comprehensive WHOIS Portal, the development of which occurred in two phases: • Phase 1 - Launch of WHOIS Informational Website (see description above in #5); and • Phase 2 - Launch of WHOIS Online Search Portal to offer a place where people could initiate a search of global WHOIS records.	√ Publication of Implementation Plan for WHOIS Search Portal Jan 2013 √ Beta Launch of WHOIS Informational Website (Phase I) – 4 Nov 2013 √ Communications Plan kicked off for Phase I – 4 Nov 2013 √ Beta Launch for WHOIS Search Portal (Phase II) – Singapore Meeting 2014 √ Communications Plan kicked off for Phase II Beta – 12 Mar 2014 √ Formal Launch of WHOIS Search Portal (Phase II) ◊ Future upgrades to include an overhaul of the Internic Service.
	Internationalized Domain Names			
12		Determine appropriate Internationalized Domain Name Registration (IRD) data requirements	The IETF WEIRDS Working Group has concluded its evaluation of technical protocols. • New Registration Directory Access Protocol (RDAP) developed; • Once adopted by the IETF, the new gTLD Registry Agreement and the New 2013 RAA will include commitments to adopt the new protocols.	√ WEIRDS finalizes new Registration Directory Access Protocol (RDAP) – Dec 2014 √ WEIRDS RDAP Protocol RFCs 7480-7484 published – Mar 2015 ◊ WEIRDS final solution to be implemented into the contracts – (TBD) √ Registrars sign new 2013 RAA (2013 - 2018); List of Registrars on the 2013 RAA available here. √ New gTLD Registries sign new registry

#				
		ICANN has remains committed to this effort. A team is currently working on the IRD requirements, but is dependent upon the conclusion of the GNSO PDP on Translation and Transliteration. Final product is dependent upon the conclusion of the GNSO PDP on translation/transliteration.	agreements. List of registries available here. √ IRD Team analysis under way √ Singapore Session on IRD Status – 26 Mar 2014 √ Interim Report of IRD Team – Apr 2014 √ Initial Model of IRD Team – Apr 2014 √ Study to Evaluate Solutions for the Submission and Display of Internationalized Contact Data – 2 Jun 2014 √ Draft Final Report of IRD Team published for Public Comment – 9 Mar 2015 ◊ Public Comment Summary – 5 May 2-15 ◊ Final Report of IRD Team – June 2015 ◊ Board Approval of IRD recommendations – estimated Mid 2015 √ Study to Evaluate Solutions for the Submission and Display of Internationalized Contact Data – 2 June 2014 ◊ Final Report – Apr 2015 See answers to #13 below.	
13	●	Requirements for Translation/ Transliteration of internationalized registration data	Issue of Translation/Transliteration is being explored as a Policy matter within the GNSO Council. Consensus policy, if produced out of the PDP and adopted by the Board, it would become binding upon the contracted parties. This output of this PDP work is required to inform the rest of the IRD related implementation work being supervised by Staff (# 12 – 14). Conclusion of this aspect of the implementation is dependent upon the speed in which the PDP can be completed once the working group is formed.	√ GNSO Preliminary Issue Report on Translation and Transliteration of Contact Information – 8 Jan 2013 √ GNSO Final Issue Report Translation and Transliteration of Contact Information published – 21 Mar 2013 √ GNSO approves the commencement of the PDP on translation/transliteration of Registration Data – 13 June 2013 √ Charter for PDP WG approved by GNSO – 20 Nov 2013 √ Initial Report from PDP Working Group on Translation and Transliteration of contact information published 15 Dec 2014 √ Public Comment on Initial Report from PDP Working Group on Translation and Transliteration of contact information – 16 Dec 2014, closed 1 Feb 2015 √ Staff Report - Summary of Public Comments– 19 Feb 2015 ◊ PDP Final Report – estimated May 2015 ◊ GNSO approval of PDP recommendations - estimated July 2015 ◊ Board approval of PDP recommendations - estimated Sep 2015
14	●	Metrics on accuracy internationalized registration data	Internationalized WHOIS Records to be proactively identified once the work referenced in #12 and #13 is complete.	IRD WHOIS Records to be proactively identified once the work referenced in #12 and #13 is complete. ◊ Scoping of requirements once the work in #12 and #13 is concluded - estimated 2015 ◊ Resources and schedule to be developed – estimated 2015 See answers to #12 and #13.
15	●	Comprehensive Implementation Plan for implementing the Final WHOIS Review Team report.	ICANN Staff developed and published its proposed Action Plan, which was adopted by the ICANN Board.	
16	●	Publication of Annual Reports on Implementation of WHOIS RT Recommendations	ICANN published its first Annual Report one year after the Board's approval of the WHOIS Policy Review Team Final Report Recommendations, with subsequent ones to be published annually thereafter.	√ Publication of first Annual Report – 4 Nov 2013 √ Publication of second Annual Report – 14 Dec 2015

WHOIS Inaccuracy Complaint Form Template

(Link:

https://forms.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form)

ICANN

GET STARTED   NEWS & MEDIA   POLICY   PUBLIC COMMENT   RESOURCES   COMMUNITY

Whois Inaccuracy Complaint Form

This form allows Internet users to submit a complaint to ICANN regarding incomplete or incorrect Whois data, including privacy or proxy contact information. The complaint is then forwarded to the sponsoring registrar, who must take reasonable steps to investigate and correct inaccurate data.

Please note: To update your own contact information, go to Correct My Whois Data to find out how.

To avoid delays in processing your complaint, please provide detailed explanation regarding each inaccuracy selected using the "Comment" field(s).

[Items with an asterisk (*) are required]

Name *

Email *

Domain Name *

☐ I do not want my e-mail address disclosed to the registrar who the domain name is registered with. If checked, please give reason below.

CQRQLG

Generate a new captcha

What code is in the image? *

Enter the characters shown in the image.

Next Page >

Contract Compliance

INTERNET GOVERNANCE

What is Contract Compliance?

The goal of Contractual Compliance is to ensure that ICANN's contracted parties fulfill the requirements set forth in their agreements with ICANN. To achieve this goal, ICANN Contractual Compliance commits to:
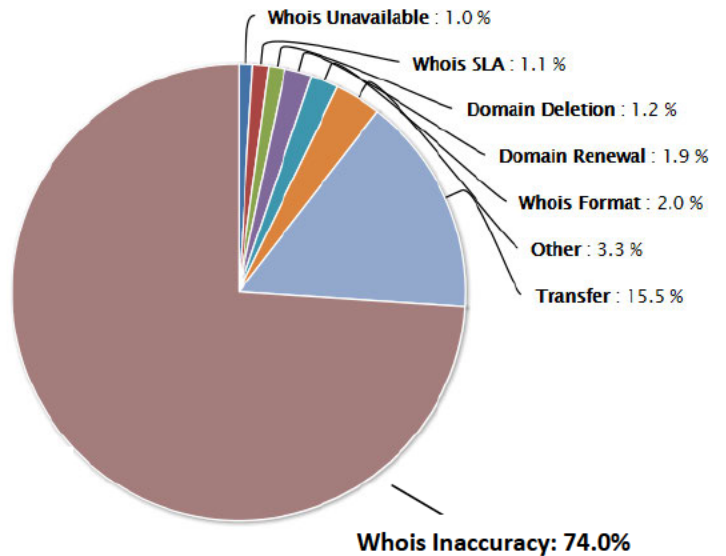
- Uphold ICANN's mission and the Contractual Compliance's vision, mission, approach; click here to learn more **About** Contractual Compliance

- Reinforce the openness and transparency of ICANN's operations, provide fair and equitable treatment to the stakeholders; click here to learn more about Contractual Compliance's **Programs**

- Maintain accessible resources for learning and reporting on compliance matters; click here for **Complaint Submission and Learn More**

- Provide clear and consistent communication on the Contractual Compliance activities; click here to review all **Reporting & Performance Measurement**

Find the appropriate link or form to file a contractual compliance complaint via this link: https://www.icann.org/compliance/complaint

Registrar Complaint Volume & Distribution

Complaint Type	October 2015	Closed before 1st Inquiry / Notice
ABUSE	39	36
CUSTOMER SERVICE	14	12
DATA ESCROW	26	-
DNSSEC, IDN, IPV6	2	1
DOMAIN DELETION	48	56
DOMAIN RENEWAL	78	40
FAILURE TO NOTIFY	2	2
PRIVACY/PROXY	2	2
REGISTRAR CONTACT	17	8
REGISTRAR INFO SPEC	15	10
REGISTRAR OTHER	5	1
RESELLER AGREEMENT	1	-
TRANSFER	636	392
UDRP	12	4
WHOIS FORMAT	81	47
WHOIS INACCURACY	3028	926
WHOIS SLA	46	47
WHOIS UNAVAILABLE	41	20
Total	4093	1604

Registrar Complaints by Category

Whois Unavailable : 1.0 %
Whois SLA : 1.1 %
Domain Deletion : 1.2 %
Domain Renewal : 1.9 %
Whois Format : 2.0 %
Other : 3.3 %
Transfer : 15.5 %
Whois Inaccuracy: 74.0%

WHAT IS A CONTRACTUAL COMPLIANCE COMPLAINT?

ICANN

THE KEY PLAYERS

Internet Corporation for Assigned Names and Numbers (ICANN) helps coordinate the world's Internet system of unique identifiers.

Type in a web address. The identifiers, ICANN helps coordinate, allow your browser to get to the right place.

Registries and Registrars
To make sure you get to the correct Internet address, ICANN has contracts with domain name registering companies (Registrars) and organizations responsible for operating Top-Level domains longer than two characters (Registries) around the world.

Contractual Compliance
Contracts are enforced through Contractual Compliance. The mission is to preserve the security, stability and resiliency of the Domain Name System and to promote consumer trust through prevention, transparency and enforcement.

Domain Name Holders
When someone has a complaint about a domain name, a registrar or registry, Contractual Compliance is often the first stop to try and resolve the complaint. Its online complaint filing system is easy to use and most users can expect a resolution within 17 days of filing.

COMMON COMPLAINTS HANDLED BY ICANN

Domain name transfer issues related to unauthorized transfers or unsuccessful transfer requests

Domain name renewal issues related to fees, renewal reminders or redemptions

Domain name registration information issues related to incorrect WHOIS data or access to WHOIS data

Registry Codes of conduct issues related to registry violation such as providing more favorable treatment to some registrars

HOW DO YOU FILE A COMPLAINT?

File a complaint online at **www.icann.org/compliance**

Ensure it is filed correctly

ICANN works with the registering organization to resolve the issue

Complete a customer satisfaction survey to help ICANN continuously improve its customer service

COMPLAINTS HANDLED BY OTHER ORGANIZATIONS

Malware – malicious code that includes worms and viruses

Phishing – an illegal attempt to steal confidential information by pretending to be a trustworthy entity in electronic communication

Private Disputes – this includes breach of contract, libel and customer service disputes

Web Hosting - various services, hardware and software for data storage

Spam – unwanted or unsolicited electronic communication

Website Content – the text, visuals and sounds users experience on a website

WHO DO YOU CONTACT?

The website address registering company

Law enforcement

Government agencies

Web hosting companies

An Attorney

If the registering company fails to comply with abuse reports requirements, contact **Contractual Compliance**

For more information, visit us at:
icann.org/compliance

To get in touch with us, email:
compliance@icann.org

EC³
EUROPEAN CYBERCRIME CENTRE
EUROPOL

The Hague, April 2014
Cyber Community Engagement
C2E Report 001-2014

C2E BITS

C2E is a thematic project focusing on Internet processes and architecture to identify the significant vulnerabilities and enablers exploited by criminals. By working together with all stakeholders including LE and Internet community, we can make the Internet a safer place for all.

Overview on ICANN's Compliance

ICANN (Internet Corporation for Assigned Names & Numbers) is the authority responsible for the coordination of the global Internet's systems of unique identifiers and, in particular, ensuring stable and secure operation.
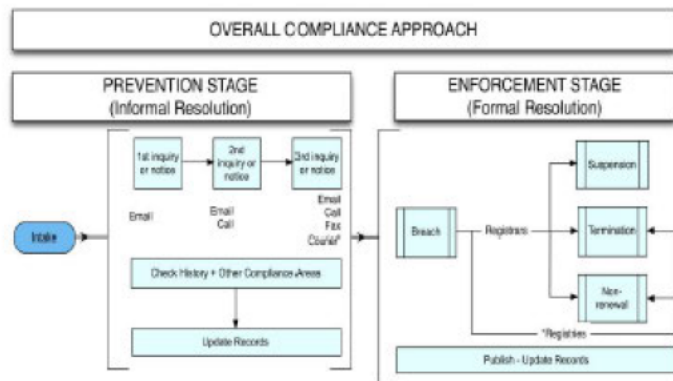
Among ICANN's roles is to implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical and administrative contact information. To ensure compliance to defined standards, a specific process is in place.

The compliance process

There are two types of agreements: with registrars (companies that register the domain name) and with registry operators, in charge of keeping a database of all domain names and the associated registrant (person or organisation who wants to open a domain name) information.

The main matter of interest regards here the agreement with registrars and their obligations.

ICANN currently has 1010 accredited registrars, each with a Registrar Accreditation Agreement (RAA). When ICANN receives complaints about registrants' WHOIS references, it has to keep registrars informed. The registrars have thus to verify the accuracy of such WHOIS data.

Figure 1: ICANN Compliance cycle. Source: ICANN (2014), http://www.icann.org/en/resources/compliance/approach-processes/overall-05mar14-en.pdf

C2E BITS

When there is a potential issue of non-compliance with WHOIS requirements, ICANN compliance team starts an inquiry, by contacting the related registrar and asking for an investigation of the situation. The issue is received through ICANN's Contractual Compliance complaint form and the full cycle for a WHOIS Inaccuracy complaint is approximately 45 days inclusive of a 15 business days response period for registrars.

During these 45 days, ICANN can send several notices if the registrar does not respond. In case the registrar does not respond after 45 days, ICANN opens a notice of breach and, later, a notice of termination, suspension or non-renewal of the contract (See Figure 1).

> *Obligations of registrars:*
>
> - *The main obligations of registrars to be compliant with ICANN are:*
> - *To provide free public WHOIS service on Port 43 and via web;*
> - *To take reasonable steps to correct inaccuracies upon notification;*
> - *To provide annual WHOIS data reminders to registrants, by verifying e-mail address and the telephone number.*
>
> *Obligation of registrants:*
>
> - *The main obligations of registrants to be compliant with registrars are:*
> - *To give accurate and reliable contact details;*
> - *To correct and update data promptly if there are any changes during the term of the registration period.*

Vulnerabilities of the compliance process

The key words in the ICANN compliance policy are collaboration, transparency and communication. However, in several case studies the ICANN compliance team is far from giving an exhaustive support to complainants.

There are four main problems in the compliance process:

- Registrants could fail to update the inaccurate WHOIS record during the 45-day complaint period (however, in this case, the registrant risks having their domain name registration suspended by the registrar);
- The 45-day period could be delayed (however, ICANN compliance team is continuously improving complaint resolution times);
- The individual Registrars could not provide evidence that it fulfils its obligation to investigate or correct the inaccuracy in WHOIS data (however, in this case, ICANN will continue to follow-up with the registrar and/or begin enforcement procedures against the registrar);
- ICANN could fail to open a breach of notice or of termination towards the non-compliant Registrar (but only under rare, extenuating circumstances).

Privacy of registrants

According to 2013 Registrar Accreditation Agreement (RAA) between Registrars and ICANN that defines the responsibilities of Registrars, an ICANN accredited Registrar is obligated to maintain a publically accessible WHOIS database that provides:

- Name and address of the domain's Registered Name Holder (3.3.1.6);

- Name, address, email address, phone number and fax (if available) of the domain name's technical contact (3.3.1.7);

- Name, address, email address, phone number and fax (if available) of the domain name's administrative contact (3.3.1.8).

The registrar has to make WHOIS information available to the public on a "WHOIS" site (here some examples: http://www.port43whois.com/; http://who.is/; http://whois.net/).

C2E BITS

It is also possible to register a domain in the name of a third party.

Registrars under the 2013 RAA are required to keep name and contact details for the domain name holder for a period of two years after the contract for the domain has been ended. All other types of data a registrar might collect (log files and billing records, IP address) must be retained for six months after the contract has ended. Such long-time requirements have been introduced to meet the law enforcement needs.

Since this public access has caused many legal issues from registrants who didn't want to make their data available to anyone, private domain registration was born. With the private registration a Registrar registers the domain in the name of a Privacy or Proxy Service Provider, not the person who is registering the domain. This allows the Registrar to put the Privacy or Proxy Service Provider's contact information in the domain contact fields, fulfilling the Registrar's obligations to ICANN yet also keeping the Registrar's customer information safe from public view.

WHOIS and criminality

After the overview along the ICANN compliance process and privacy-related system, it is relevant to understand how a criminal could take advantage of compliance vulnerabilities or of privacy statements.

WHOIS system is the matter of concern for crime-related events. The ICANN compliance process can indeed be a matter of interest for law enforcement as long as there is a misuse or abuse of WHOIS data and there is not a ready and effective response by ICANN authority.

There are three main cases of misuse/abuse of WHOIS data:

- Cybercriminals who make an improper use of others' WHOIS data: use of publicly accessible personal data to spam, to harm (malware delivery) or to harass individuals. This kind of misuse is linked with the wider debate on WHOIS data privacy, because registrants need to protect their data from prowlers;
- Criminal registrants who give false WHOIS credentials to Registrars to avoid identification, for instance in order to conduct illegal or harmful Internet activities (hosting child abuse sexual images, advanced fee fraud, online sale of counterfeit pharmaceuticals);
- Criminal registrants who make use of the private domain registration (domain names registered via privacy or proxy services or offshore) to obscure the perpetrator's identity. In some cases these companies allow for crypto currencies, digital currencies and c-coin payment options. This system could both help criminals to disguise their identities (e.g. Bitcoin system guarantees anonymity of buyer and seller through IP address anonymity) and to carry out money laundering activities.

Law Enforcement implications

The challenges of the Internet era are becoming more and more serious. The growth of cyber-related crimes, of alternative payments method and of customers' privacy claims affects ICANN's approach to WHOIS data protection. There is a broad need of continuously improving ICANN regulations by focusing on new threats and their possible solutions. Law Enforcement can have access to publicly accessible WHOIS data as well as to information managed by Registrars.

As ICANN's governing contracts and compliance processes strive to provide a solution targeting the inaccuracy of WHOIS data, Law Enforcement will benefit from being informed on the most common and extreme WHOIS inaccuracy cases ICANN deals with. The effectiveness of the ICANN compliance process becomes thus relevant to help Law Enforcement in fighting against potential criminals.

For comments, feedbacks and further discussion: EC3 SPACE EPE

IANA Transition

A Short Overview

In March 2014, the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) announced its intention "to transition key internet domain name functions to the global multistakeholder community."

This process is of importance to public policy interests as it constitutes a move away from the contractual relationship between NTIA and ICANN, which contained a number of key provisions including a commitment on WHOIS accuracy. It remains to be seen how these provisions will be maintained and enforced in the future. Furthermore, in the transition process, the possible future roles of current key actors are being evaluated and may be reshaped.

What does the transition mean in practice? NTIA's responsibility includes the procedural role of administering changes to the authoritative root zone file – the database containing the lists of names and addresses of all top-level domains – as well as serving as the historic steward of the DNS. NTIA currently contracts with ICANN to carry out the **Internet Assigned Numbers Authority (IANA)** functions and has a Cooperative Agreement with Verisign under which it performs related root zone management functions. Transitioning NTIA out of its role marks the final phase of the privatization of the DNS as outlined by the U.S. Government in 1997.

NTIA has communicated to ICANN that the transition proposal must have broad community support and address the following four principles:

- Support and enhance the multistakeholder model;

- Maintain the security, stability, and resiliency of the Internet DNS;

- Meet the needs and expectation of the global customers and partners of the IANA services; and,

- Maintain the openness of the Internet.

While stakeholders work through the ICANN-convened process to develop a transition proposal, NTIA's current role will remain unchanged. The current IANA functions contract expires September 30, 2016.

See https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions for more information.

Shortly after the NTIA Announcement of 14 March 2014, ICANN launched a multistakeholder process and discussion to gather community views and input on the principles and mechanisms for the transitioning of NTIA's stewardship of the IANA functions.

Following a month-long call for input on the community-driven draft proposal, on 6 June, ICANN posted the Process to Develop the Proposal and Next Steps.

Then following a call for names, the IANA Stewardship Transition Coordination Group (ICG) was formed comprised of individuals selected by each represented community. In October 2015, they delivered a proposal to be sent to the NTIA recommending a transition plan of NTIA's stewardship of IANA functions to the Internet community, consistent with the key principles outlined in the NTIA March 14 announcement.

This proposal consists of three parts: The numbers and protocol parameters and the names portion. While the numbers and protocol parameters parts are complete, the names portion of the proposal is conditioned on ICANN-level accountability mechanisms currently under development in the Cross Community Working Group on Enhancing ICANN Accountability (CCWG). Before sending this proposal to the NTIA via the ICANN Board, the ICG will secure confirmation from the CWG that its accountability requirements have been met. This process is currently ongoing.

Further information is available at: https://www.icann.org/stewardship