Summary of Public Comments to the WHOIS Policy Review Team's Discussion Paper

This document provides a summary of the comments received from 9 June to 23 July 2011 in response to the request for public comments on a Discussion Paper, issued by the WHOIS Policy Review Team and featuring 14 questions. The comments are grouped per question referenced and listed by contributor in chronological order of submission. Comments not referring to any specific question are grouped under "Other Comments", at the end. The original contributions should be consulted for complete information. In total, 29 comments were submitted by 27 contributors. The comments are hyperlinked below for easy access and available at: http://forum.icann.org/lists/whoisrt-discussion-paper/

Contributions provided by (in alphabetical order, by abbreviation)

AFNIC	AFNIC	InterContinental Hotels Group	IHG
At-Large Advisory Committee	ALAC	International Trademark Association –Internet Committee	INTA
Business Constituency	BC	Intellectual Property Constituency	IPC
Brendan Stephenson I II	BS	Milton Mueller	MM
CIRA	CIRA	Michele Neylon	MN
CNCERT/CC	CNCE	Motion Picture Association of America	MPAA
CNNIC	CNNIC	Non-Commercial Users Constituency	NCUC
Coalition for Online Accountability	COA	Nominet	NOM
Christopher Wilkinson	CW	Patrik Klos I II	PK
Edward Lassotovitch	EL	SIDN	SIDN
Fatima Cambronero	FC	Simon Lange	SL
Frank Ellerman	FE	Time Warner International	TWI
Hogan Lovells	HL	Valentin Höbel	VH
International Anti-Counterfeiting Coalition	IACC		

RECOMMENDATION/CONCLUSION	SUMMARY OF COMMENTS
1. What measures should ICANN take to clarify its existing WHOIS policy?	**FE:** Billing, law-enforcement or marketing info in public WHOIS data are not mandatory, but must be correct if present. WHOIS is mainly a last option to obtain contact info if all other ways fail. Public WHOIS data is primarily intended to help domain owners in case of technical problems. ICANN should help registrars communicate this purpose to registrants. **VH:** Remove all personal data and revoke the duty to provide personal data. Introduce a data field with an e-mail address of the registrar who forwards messages to the owner. Remove the annual reminder for registrants to keep their data up to date. **IHG:** ICANN should live up to its commitment to provide open access to accurate registrant information. Proliferation of false WHOIS data undermines ICANN's legitimacy and allows an increase of misleading activities online. Registrars should verify registrants' WHOIS data.

	INTA: ICANN should clarify its existing Whois policy and educate the public and contracted parties on the importance of the Whois policy and of compliance. The Whois policy should be clearly described on the ICANN homepage so the public can understand its purpose and the roles, rights, and responsibilities of all stakeholders. ICANN should describe the implications of providing false or misleading Whois information. A link should be created on the ICANN homepage to the WDPRS and ICANN should take other measures to inform about the WDPRS through educational programs and publications. ICANN should provide staff support to ensure system performance. **IACC:** Assurance of public access to complete, accurate and up-to-date WHOIS data is a core responsibility of ICANN, as restated in the AoC. ICANN has proved deficient in its enforcement of registrar obligations to collect such data and make it accessible. ICANN's compliance efforts amount to "too little, too late". ICANN must fulfill its promises, with emphasis on compliance, and publish policies with the intention to fulfill WHOIS obligations. Changes should be published widely so registrants get adequate notice that their domains are jeopardized if they fail to provide true, accurate and complete WHOIS data. Registrar responsibilities for WHOIS must be clearly articulated. An advisory on registrar deployment of proxy services is a helpful first step. **TWI:** The Whois policy can be discerned from the documents listed in the Discussion Paper and paragraph 9.3.1 of the AoC encapsulates the main objectives. ICANN has sought to implement this policy through contractual arrangements with gTLD registries and registrars. The Review Team should evaluate how well those arrangements advance the basic goal, and how effectively ICANN is enforcing compliance. We urge the Review Team to focus on these areas, rather than on articulating a comprehensive statement of policy in this area. **CW:** The initial purposes of Whois did not extend to the current utilization. More is expected of Whois than it is capable of delivering. Registries and registrars could be obliged to provide verified data about specific domains for which a request had been made. Applying current Whois policy to IDN registries is not obvious. **MPAA:** ICANN should establish WHOIS accuracy metrics, see NORC study for examples. Currently, there is no requirement to verify registrant name and address, nor to determine if country and region code of the phone number correspond with the address. We recommend a single, cross-referenced registry database and a registrant ID. A central database for all registrant data could be used could be used to cross check submitted contact information against existing registrations. If there are inconsistencies, the application and existing registrations could be placed on hold pending verification. These cross checks could query online resources like telephone directories, mapping programs, and credit check services, for which the applicant could pay the fee. A registrant should receive an ID number and a PIN by a trusted entity after verification. Verification could include a government issued ID card, a due diligence telephone call, or an online credit check. The ID would be submitted when applying for new domains or for renewal of an existing domain. **COA:** The documents listed in the Discussion Paper outline clearly what the community requires from Whois: that registrant contact data be publicly accessible through multiple channels, without charge or undue restrictions, and that data be current, complete, and accurate. This is the Whois system that ICANN inherited, but its stewardship has fallen short and the Review Team should issue recommendations to improve stewardship and to realize the full potential of Whois for consumers, law enforcement, right holders, and the public at large. **IPC:** Public access to complete, accurate and up-to-date WHOIS data is ICANN's responsibility, stated in the original MoU and restated in the AoC, but ICANN has not fulfilled its promises in this regard. ICANN must clarify its WHOIS policy and implement it effectively. ICANN should educate the community about WHOIS and the consequences of failing to provide correct data. ICANN must bring gTLD registries into the effort to improve WHOIS, not only attempt to fulfill its WHOIS commitments through provisions in the RAA. ICANN must emphasize contract compliance, including allocation of resources to compliance, publish policies that demonstrate the intention to fulfill WHOIS obligations, and reform proxy registration services. These changes should be widely published so that registrants notice that their

	registrations are in jeopardy by non-compliance with WHOIS requirements. The registrars have been reluctant to see clearer articulation of its obligations but the AoC commitments must override that. Efforts to provide registrar guidance with an advisory regarding proxy services is a helpful first step. RAA provisions on proxy services must be reformed to enable prompt disclosure of data in cases of abuse. **PK:** State the intent of the WHOIS policy, including why registrars are required to collect and present valid WHOIS data for each domain. **HL: T**he policies are concise but the obligations could be made clearer. ICANN must implement WHOIS policy more effectively and ensure compliance. Proxy services should have to ensure prompt disclosure in case of domain name abuse. The WDRP should prompt a registrant commitment to confirm WHOIS accuracy. Failure to confirm could constitute grounds for cancellation. The Restored Names Accuracy Policy should state a definition of "accurate" information and how registrars should ensure that information is accurate. The procedure for handling WHOIS conflicts with Privacy Law appears to allow a case-by-case analysis. ICANN should provide a report with the statistics of recourse to this procedure. ICANN could also consider outreach to registrars to remind them of their RAA obligations for WHOIS. **FC:** WHOIS predated ICANN and was not established as a written policy. There is the RFC 3912 WHOIS protocol and a number of ICANN policy documents, but an easily accessible uniform WHOIS document is needed so users understand the policy. **BC:** In the AoC, ICANN committed to a number of WHOIS obligations and the 2007 GAC WHOIS Principles emphasized the importance of WHOIS accuracy to ensure Internet security and stability, with subsequent GAC documents stating compliance concerns. However, ICANN lacks a comprehensive WHOIS policy and many RAA provisions are weak or unclear (see submission for details). ICANN cannot live up to its AoC commitments unless all stakeholders are required by contract to ensure the accuracy of WHOIS data at all stages of the domain name process. The BC recommends that a) the RAA be amended to require contracted parties to verify the accuracy of WHOIS information. Other industries have employed successful online data verification systems to ensure accuracy of information. Registrars already gather accurate information regarding credit cards and other forms of payment. Valid WHOIS data should equally be a prerequisite to complete a registration. b) ICANN should develop guidelines for contracted parties and registrants informing them about data elements considered valid for WHOIS and processes for verifying WHOIS data. c) ICANN should amend the RAA or develop guidelines instructing registrars how to correct false and inaccurate WHOIS data, including a regular practice of cancelling registrations in appropriate circumstances. d) ICANN should also consider a centralized WHOIS database. Graduated sanctions should ensure compliance with WHOIS obligations.
2. How should ICANN clarify the status of the high level principles set out in the Affirmation of Commitments and the GAC Principles on WHOIS?	**LE:** See answer under 1 above. **VH:** See answer under 1 above. **IHG:** IHG appreciates ICANN's bottom-up policy processes, where brand holders have led WHOIS discussions. WHOIS policy embodies ICANN's commitment and should be strengthened. ICANN should ensure that registrars accept liability for false WHOIS data. **INTA:** ICANN should take measures to ensure all Internet stakeholders, including contracted parties, are informed of the importance of Whois and their obligations. ICANN must bolster its contractual compliance activity to meet its AoC obligations. **TWI:** See answer under 1 above. **COA:** See answer under 1 above. **IPC:** ICANN must publicly state its dedication to the policies articulated in the AoC and make more vigorous compliance efforts. Concrete implementation of the AoC goals should take precedence over drafting a single document with all Whois policies. ICANN must enforce registrant compliance through measures designed to terminate registrations with false data. The RAA should be amended to spell out the responsibility of registrars to terminate registrations in appropriate cases. ICANN compliance should monitor and report on how registrars exercise their current discretion in dealing with registrants. Registrant rights can be protected through notice and cure provisions.

	PK: Can't really say since I haven't read them. **HL:** Provide a detailed definition of the principles and link them to registrar WHOIS obligations as part of the RAA. This would strengthen and clarify these principles, linking the importance of enforcement of the principles to effective actions against inaccurate WHOIS data. Compliance efforts need to be increased against registrars who fail to comply and registrants who fail to provide accurate WHOIS data. **FC:** Preparing a Beginners Guide on WHOIS Policy. **BC:** ICANN must create accountability mechanisms that are specific and measurable. ICANN should undertake a full audit of the WHOIS record set and measure it for accuracy. Third parties have already volunteered to assist in that effort. That audit, combined with studies on inaccurate WHOIS data, would set a baseline for measuring ICANN's compliance with its AoC obligations. ICANN must require contracted parties to live up to their WHOIS obligations, including correcting inaccurate WHOIS data. ICANN must beef up WHOIS enforcement, while allowing flexibility for the way in which registrars comply with their obligations. A public WHOIS dashboard could show performance.
3. <u>What insight can country code TLDs (ccTLDs) offer on their response to domestic laws and how they have or have not modified their ccTLD WHOIS policies?</u>	**LE:** National laws may prohibit mandatory contact data in public WHOIS but not voluntary data. Registrars selling domains in these ccTLDs can communicate why not publishing voluntary data will result in no trust for, e.g., anti-spam applications. **VH:** See answer under 1 above. **MN:** Many European ccTLDs offer a public WHOIS service with limited non-technical information, while law enforcement can access full details. A distinction is made between personal and business domain registrations, for example in .IE. In both cases no personal data is available in WHOIS. In .CO.UK, the WHOIS output shows if a registrant has "opted out", but a company would not have that option. While a business domain does have more data published in WHOIS there is no email address or phone number. Under .EU, WHOIS is limited to technical details and shows more information about a business domain, while a personal one's output is limited to an image of the email address, not accessible to bots. The only gTLD that has followed a similar model is .TEL, where registrants can opt out in a way similar to .CO.UK and the WHOIS output is minimal, while a business registration is more detailed. *See submission for multiple and detailed examples*. **AFNIC:** AFNIC's data publication and access policy describes how registrant data is gathered, disclosed and used during the lifetime of a domain name registration: a) Private registrants' data is not displayed in the public Whois b) AFNIC provides on line web forms to enable any interested party to send electronic messages to the domain name admin contact without disclosing its data c) Right owners or affected parties may request disclosure of registrant data. Such requests are handled by AFNIC which checks whether the affected party has some right over the domain name before disclosing. This policy was set up in 2006 with amendments in 2007 to comply with privacy laws and an instruction from CNIL. While .FR approached 2 million domains in 2010, AFNIC handled 412 data disclosure requests, whereof 356 granted. The policy reinforces trust from private registrants, as they can provide accurate data with limited risk of unsolicited communications, and customer relations suggest that the policy has a positive impact on data accuracy. **INTA:** Most ccTLDs provide the entire Whois record at the registry level, while some provide the entire record only to certain groups such as law enforcement agencies, certification authorities, and registrars that need access for administrative purposes. The extent of information that is shared is generally determined by local law. DENIC publishes all contact information, and German law requires the contact information to be placed on the website if engaged in business. France has a similar requirement. Where there is a need to balance local privacy laws with access to full Whois, mechanisms to improve transparency can be considered, as in the Netherlands. A thick Whois model has been employed in many new gTLDs for years without legal problems or objections from national authorities on privacy grounds. ICANN has a procedure, that a registry can invoke when facing a conflict between its Whois obligations and national privacy laws (see, http://www.icann.org/en/announcements/announcement-18dec07.htm). To date, this procedure has never been invoked.

	TWI: Time Warner commends the Review Team for looking to the Whois experience of ccTLDs, even though ICANN plays only a limited role in this area. ccTLDs may have much to teach the gTLD world in improving Whois accuracy , for example by registrant data verification. **CNNIC:** We provide public WHOIS service with basic and concise information. Registrant information is reachable through the provided WHOIS information. Meanwhile, complete internal WHOIS information can be accessed on LEA request. By doing so, we both protect our registrants' privacy and support legal enforcement. **NOM:** The .UK WHOIS policy was developed in consultation with stakeholders and the Information Commissioner's Office. It meets the requirements of UK law and good practice, protecting the privacy of personal information for non-trading individuals. The .UK WHOIS does not contain the same details as required for gTLDs. It lists: Domain name, Registrant, Registrant type, Registrant's address, Registrar, Relevant dates, Registration status and Name servers. We provide a service, PRSS, for searching domain names, registrants and similar names. PRSS has a web interface, allows use of wildcards and is available to anyone based in the EEA on a contract-only basis. It is aimed at in-house counsel, law firms, brand protection agencies etc, although LES and the Internet Watch Foundation have access. **IPC:** Some ccTLDs have implemented WHOIS data verification protocols that may deserve studying. ccTLDs for countries with privacy laws have experience in balancing data privacy restrictions with the need for accurate WHOIS data to law enforcement professionals, civil litigants and other requesters. ccTLDs that have thick WHOIS may provide insight into whether this leads to more accurate WHOIS data. The experience of ccTLDs that regulate or prohibit proxy registration services should be studied for models applicable to gTLDs. **PK:** If a country has stricter privacy laws than the US, that should have no impact on WHOIS policies controlled by ICANN. Companies should not have privacy in WHOIS records as only shady businesses need privacy to hide from the authorities. For personal use domains, a registrar may provids a form of privacy to the owner, but the information in the WHOIS record must contain a valid email address and phone number for access to someone who can act on technical or security issues, or get in touch with the owner in a timely manner. **HL:** Among ccTLD registries responding to EU data protection legislation, both .EU and .FR differentiate between corporate bodies and private individuals. The .EU WHOIS policy states that full data is displayed for corporate bodies, but data displayed for private individuals is limited to the email address in an image format to avoid data mining. Disclosure of full WHOIS data for private individuals to third parties is subject to requests stating legitimate reasons. .FR also differentiates the public WHOIS data between corporate bodies and private individuals. The latter can request a "restricted disclosure" meaning that no personal information is disclosed and only available to third parties on grounds of a judicial order or upon a request detailing the reasons. Although the approaches are legitimate and the systems in place allow for prompt disclosure, they create an extra burden for rights holder who incur extra costs and lose time when trying to address abusive registrations. This system also prevents rights holders from identifying patterns of illegitimate registrations since the restricted disclosure of data applies to the public WHOIS as well as to data provided to professionals. Rights holders incur the risk of action by these registries if they consider that the disclosure was illegitimate, therefore reversing the liability from potential infringers to rights holders. **BC:** A ccTLD aspect to consider is whether accuracy is improved by having "thick" WHOIS data maintained at the registry level. **CIRA:** Any WHOIS policy must reflect that a registry has to comply with local law. ccTLDs are clearly subject to local laws, and gTLDs must also comply with applicable laws, which may include privacy laws. CIRA policies are subject to local law, and take into consideration privacy and other best practices.
4. <u>How can ICANN balance the privacy concerns of some registrants with its commitment</u>	**LE:** Privacy proxies are not a problem for the primary purpose of WHOIS. Hiding e-mail addresses of domain owners who cannot resolve technical issues with their domain is a "good thing", but third parties should be able to find a technical contact. **VH:** Allow proxy services and introduce the possibility for registrars to provide such a service. Personal data should only be provided to the

to having accurate and complete WHOIS data publicly accessible without restriction?	registrar and not be public. The registrar may only disclose registrant personal data to local authorities. Domain owners should be able to provide personal WHOIS data if they want to. The need for accurate WHOIS data may not overrule the domain owner's need for privacy protection. Full WHOIS data may be publicly accessible for domains which are owned by companies, authorities and institutions. **MN:** I don't think it can. There are many valid reasons why a registrant may wish to keep some of their data private. I'm also not convinced that making complete WHOIS data available without restriction is such a good idea. **IHG:** There must be a reliable access route to domain registrants, for multiple reasons: 1) Individual consumers, with concerns about their own information have a right to contact domain name administrators with questions and concerns. 2) Complete and accurate WHOIS data promotes consumer confidence in online business. 3) Trademark owners with infringement claims have a right to contact the registrant directly. Direct negotiation could save the time and cost for dispute resolution process. 4) Immediate access to information is an asset for LEA, particularly in pursuit of fraud activities. Barriers to open information trigger due-process requirements before officials can obtain information and act. This could decrease overall user confidence in the safety of the internet. Current restrictions on bulk queries of WHOIS data reasonably protect registrants from massive spamming, and helps ensure that the data will be used for legitimate purposes. **INTA:** INTA supports open Whois access to accurate ownership data for addressing legal and other issues with any domain name. Data should include the owner's identity and accurate contact details. Publishing on the Internet is a public act, and the public should be able to determine who they are dealing with. This is important for domains with commercial content, or registered by entities, where privacy interests are limited or nil. Open access should be the default and for domains registered using a privacy or proxy service, there should be procedures for relaying communications to the owner and for revealing registrant data to a party who has evidence of actionable harm. **IACC:** It is not ICANN's responsibility to balance privacy concerns given its commitment to providing accurate and complete WHOIS data. Any effort to vitiate that obligation would undermine ICANN's commitment. ICANN must accept that WHOIS does not implicate privacy concerns given all the options to engage in free speech without registering a domain name, and that the balancing issue is a matter for other entities. ICANN could quell privacy concerns by emphasizing that anonymous actions on the web are still possible but violations can best be stopped by tracking down the holders of the offending domains. ICANN should highlight that most sectors require accurate information for business licenses, trademark registration, and other services; domain name registration should be no different. The policy can be clarified by assuring that abuse will not be tolerated, and that WHOIS only serves constructive purposes that can prevent web-related offenses and fraud. ICANN should inform about existing security measures, including implementation of rate-limiting systems. **TWI:** A troubling trend is the proliferation of proxy registrations of gTLD domains, and ICANN's inability to bring these in line with its policy goals. The ability to contact the registrant depends on whether the proxy provider decides to disclose information. Not all providers are responsible and divulge information when presented with evidence of abusive activities. While proxy registration may be justified in limited circumstances, the existence of some 20 million gTLD domains with inaccessible registrant data is contrary to the WHOIS policy goal. Unless ICANN brings proxy registrations under some degree of control, its claim to responsible stewardship of Whois will ring hollow. This failure is largely due to an inadequate RAA, identified by GNSO as a top priority for revision. However, in a recent GNSO Council vote, registries and registrars blocked progress on this revision. A modest proposal to issue a registrar advisory on the applicable language in the RAA met opposition from registrars and was never implemented. The Review Team should note the proliferation of proxy services as a major flaw in ICANN's implementation and recommend corrective steps, like clarification and enforcement of the RAA provisions on licensing of Whois data, revision of the RAA to address this more effectively, and requiring thick Whois across the gTLD space. Voluntary "best practices" guidelines for registrars may have a role to play, but are unlikely to be meaningful absent the steps above. Some registrants have legitimate

	privacy concerns which may be at odds with the Whois goals, but the scope of these concerns has been exaggerated and mechanisms are already in place to help registrars or registries to manage conflicting legal requirements. Further adjustments to the implementation of ICANN policies may be called for to address specific privacy concerns, but experience shows that proxy registration is not the solution. **NCUC:** Privacy and accuracy are connected as some registrants use "inaccurate" data as a means of protecting their privacy. Other options to keep this information private may make registrants more willing to share accurate data with their registrar. The problem for many registrants is indiscriminate public access to the data, as the lack of any restriction implies an unlimited potential for bad actors to access and use the data. WHOIS access must give natural persons greater latitude to withhold or restrict access to their data. That position is consistent with EU data protection law and has even been advanced by FTC and FBI in the US. The NCUC recommends reviewing the WHOIS Task Force proposal for an Operational Point of Contact (OPOC), where registrars would publish the registrant's name, country and state/province together with contact information for the OPoC. Registrants with privacy concerns could name agents to serve as OPoC, thereby keeping their personal address information out of the public records. *See submission for multiple references.* **CW:** Unrestricted public access to personal data for individual registrants in Whois infringes EU privacy laws. Accordingly, the AoC qualification that ICANN should enforce Whois policy "subject to applicable laws" exempts registrars and registries in EU/EEA jurisdictions from those policy provisions. However, this begs the question which rule to apply if the registrant is in such a jurisdiction but not the registry nor the registrar. ICANN has a procedure for handling Whois conflicts with privacy law and it would be interesting to learn how many times this procedure has been invoked, and what decisions ICANN has taken as a result. **MPAA:** Most countries require businesses and other entities to provide accurate information in dealing with authorities and the same should apply to Whois data. Some countries have privacy laws affecting the display of ccTLD WHOIS data, but an issue is which laws to apply when a company responsible for registration services for the ccTLD is based in another jurisdiction, e.g. .TO is assigned to the Island of Tonga, yet the company handling the registrations for .TO domains is located in California and does not maintain a public Whois. **CNNIC:** ICANN should promote the enhancement of WHOIS accuracy, but WHOIS policies should respect national laws and regulations in different countries. ICANN should request accurate and complete WHOIS data, but give flexibility to registries/registrars to show tailored WHOIS data to the public, based on national privacy laws. By doing so, some balance could be achieved. Accurate and complete WHOIS information would still be available when necessary, e.g. for LEA; while basic WHOIS service would be available for proper use. **NOM:** In line with UK data protection law, a registrant who is a non-trading individual can opt to have the address omitted from WHOIS. Non-trading is interpreted strictly - the domain should not be used for any revenue-earning activities. If a domain name is incorrectly opted out, we opt it back into WHOIS and lock it to prevent renewed opt-out. We may suspend the domain for breach of terms and conditions. **COA:** There is already a mechanism for resolving conflicts between registrars' (or registries') contractual obligations and privacy laws, and no need for further policy development in this area. Registrants may also require privacy protection in special circumstances, e.g. to carry out political dissident activities in a repressive society. This category of registrants should be accommodated, but the scope of the problem has been exaggerated as there are multiple options to establish an online presence for disseminating views that do not involve registering a domain name in a gTLD, for example thru social media. A repressive state would furthermore have other means than WHOIS to identify dissidents. Further discussions should determine the scope of this problem and identify solutions, but tens of millions of anonymous domain names, just a fraction of which are used for the special circumstances above, is an irrational "solution" that inflicts greater costs than warranted upon legitimate e-commerce, consumer interests, law enforcement and the public at large. That is the "system" now in place, due to widespread proxy registration and unenforced Whois accuracy obligations. That "system" must be fixed.

	IPC: ICANN is committed "to having accurate and complete WHOIS" while the GAC Principles state that WHOIS service should provide "sufficient and accurate data about domain name registrations and registrants subject to national safeguards for individuals' privacy." ICANN is not required to implement safeguards for individuals' privacy, the burden of restricting access to such data in a particular locality falls on the locality. ICANN has a procedure for registrars or registries exposed to liability under privacy laws if they fully comply with their Whois obligations. Global norms about identification data for commercial entities make such entities unlikely candidates for WHOIS data privacy. Proxy services provided to individual registrants in accordance with best practices can satisfy the desire of individuals for WHOIS data privacy. There may be special cases in which particularly vulnerable individual registrants need to be treated exceptionally with regard to the otherwise general obligation for full public access to Whois data. This is an area in which ccTLD experience may be instructive. **PK:** See my answers to 3. **HL:** Striking an appropriate balance between privacy rights of individuals and right holders' interests is essential. The use of thick WHOIS has not led to abuse for which solutions have not been found. The RAA makes it clear that the registrar must inform registrants about the purposes personal data will be used for, the data recipients and how data can be accessed and modified. A registrar best practice for dissemination of this information to registrants would be useful. Adopting a system like .EU and .FR would be excessive as it imposes burdens on rights holders and require resources dedicated to requesting disclosure of registrant data. Such a system may prevent investigation of illegitimate registration patterns and render UDRP provisions moot. Domain names used for commercial purposes should not be allowed to use a proxy service, and should have WHOIS data public, while an individual expressing ideas, with no commercial benefit sought, could justifiably benefit from a proxy service, or a protection as per .EU or .FR. **FC:** Balancing privacy, security and the right to know means to identify minimal data requirements that allow quick identification, like Registrant Name, State/City/Country, email and telephone. The rest of the data gathered should be managed according to national legislation on privacy and data protection. However, not every country has legislated on privacy and data protection. There should be a global study on privacy law to find a model that suits everybody (if possible), with guidance from OECD and UN. **BC:** The GAC Principles note that WHOIS should provide "sufficient and accurate data about domain name registrations and registrants subject to national safeguards for individuals' privacy" in a manner that supports the stability, reliability, security and interoperability of the Internet and facilitates continuous, timely and world-wide access. There must be a balance that allows access to accurate WHOIS information while building in any processes to address privacy concerns. Most countries require businesses to provide accurate information when they apply for a business license, tax-exempt status, or inclusion in a directory of trademarks. Some countries have established that their privacy laws apply to the display of country code WHOIS data. **CIRA:** Accuracy, completeness and privacy are not mutually exclusive. It is possible to have a fully accurate and complete database that also respects privacy. A system with mandatory disclosure of WHOIS information may undermine the goal of accuracy and completeness as it may encourage the use of proxy and privacy services. For this reason, it is worthwhile considering some level of privacy, under appropriate circumstances, in conjunction with appropriate disclosure mechanisms.
5. <u>How should ICANN address concerns about the use of privacy/proxy services and their impact on the accuracy and availability of the WHOIS data?</u>	**LE:** See answer under 4 above. **VH:** Allow proxy services. **MN:** If ICANN addressed individuals' privacy concerns, many issues with privacy/proxy services would probably disappear. **IHG:** Privacy services frustrate protection of brands online, which leads to confusion and problems for consumers. Proxy services have become a tool for registrants to avoid making information available to the public. It is not our position to halt these services entirely,

	provided proxy providers maintain accurate registrant data and make that information timely available in case of a legitimate request. The studies of proxy services and their use will be influential in moving forward on this issue. *See submission for case references*. **INTA:** Where a domain has been registered using a privacy or proxy service, there should be mechanisms for relay of communications to the registrant, and for revealing registrant data upon a justified request in line with RAA provisions. Due to the high degree of non-compliance with these provisions, privacy/proxy services should be governed by rules overseen by ICANN, including relay and reveal processes. Privacy/proxy services would have to assent to these and affirm compliance in annual statements to ICANN in order to operate. **IACC:** ICANN did attempt to address the use of proxy services, with a draft advisory including best practices for the use of proxy services while reconciling with third party needs for WHOIS data. If such an advisory cannot be adopted in a manner consistent with ICANN's contractual relationships, further RAA amendments must be done to minimize the potential for abuse of the WHOIS system through proxy services. More frequent meetings between the ICANN staff and the GAC would also be beneficial to inform GAC of ICANN policy agendas. Multilingual access to Whois would call for further involvement from GAC members, which in turn would promote consensus. **TWI:** See answer under 4 above. **NCUC:** ICANN should recognize that privacy and proxy services fill a market need; the use of these services indicates that privacy is a real interest of many registrants. Concerns about the use of these services are unwarranted. **MPAA:** Proxy/privacy providers supply contact information to a registrar in lieu of registrant data, leaving Whois to identify a proxy service, not the registrant. Suspects seek these services to conceal their identities and many providers operate in a dubious way, being unreachable or not responding to inquiries. The time lapse before data is disclosed gives the suspect ample time to transfer the domain to another suspect entity or otherwise evade detection. We recommend registering and accrediting privacy/proxy companies and prohibiting registrars from accepting registrations from unaccredited proxy providers. As part of the accreditation process, ICANN must require providers to run checks on the applicant's contact data and provide a referral process to parties to disclose registrant data. Failure to disclose this information or perform checks would result in loss of accreditation and public disclosure of all Whois data collected. ICANN-mandated best practices should include a protocol for proxy services to use in responding to requests for registrant data, along with a requirement to provide an abuse point of contact, contact information and physical address of the proxy service. **NOM:** We do not recognize the use of privacy and proxy services. Our contract is with the party that is identified as the registrant. We do not have figures on the use of privacy services, but the provision of an opt-out for non-trading individuals and the fact that email and phone numbers are not in the public WHOIS reduce the need for such services. We would expect a company to use its business trading address or registered office. A sole trader working from a private address might opt to use a third party: we could probably not identify where this was being done. Registrants risk losing their domain names if they cannot be contacted through the listed WHOIS address. **COA:** ICANN must bring order, predictability and accountability to proxy registrations in order to improve accuracy of Whois data, so the service can fulfill its function. COA does not reject the concept of proxy registration in principle, but we encourage the Review Team to study the experience of ccTLDs (such as .us) that do not permit it. There may be legitimate reasons, in limited circumstances, why registrants should be permitted to submit contact details of a third party. Bona fide registrants may well use such a service, but it will inevitably prove attractive to registrants who engage in rights infringements, fraud, or other misconduct. In the experience of one COA member, the majority of sites investigated for high-volume copyright infringement are registered using proxy services. The key is whether a member of the public can gain timely access to the registrant data when it has a bona fide need to do so. The current system is inadequate and section 3.7.7.3 of the RAA is weak and ambiguous. Aggressive enforcement, while needed, will provide only limited benefits. Even

	modest efforts to clarify it through a proposed Advisory have collapsed under opposition from registrars. Whether a third party who presents a justified request to the proxy provider will get the registrant data varies wildly. Reform of the proxy registration system is long overdue and the Review Team should call for such reform as a matter of priority. ICANN could accredit proxy providers, set ground rules for their operation and prohibit registrars from accepting registrations by unaccredited providers. A first step may be to focus on proxy services offered by accredited registrars or their resellers, requiring them to verify contact data from the registrants and keep this data current, to disclose registrant data upon a justified third party request and to respect firm time limits for response. These requirements would be enforceable against registrars, subsidiaries, affiliates, or resellers. Registrars would face enforcement action if they deal with non-affiliated proxy services. A code of best practice among responsible accredited registrars would be at least as effective a way to reform the proxy registration system as RAA amendments, provided all registrars sign up to the code. *See submission for examples and models.* **IPC:** There are critical failures associated with proxy services, which now account for one-fifth of all gTLD registrations. There are many inappropriate uses of proxy services by registrants and registrars, as well as wide variances among proxy services in responsiveness to LEA and third parties request for data disclosure. ICANN should create guidelines and best practices for privacy/proxy services. Registrar cooperation in the development of guidelines and best practices should be actively solicited; but the refusal of some or all registrars to participate cannot justify delay. Given the critical failures and the ambiguity of relevant provisions, RAA amendments are also needed. **PK:** ICANN should require that the email addresses and phone numbers are accurate. It is criminal to put an auto-responder on an admin or technical contact and irresponsible for a technical contact to have a pattern-matching spam/phish filter on their mailbox, as that may prevent people from informing about a domain that has been hijacked or hacked! **HL:** Section 3.7.7.3 of the RAA addresses the obligations of the proxy provider as the Registered Name Holder for a domain, with liability resting with them if they fail to disclose the contact information. However, the ambiguity of certain RAA provisions and increasing use of proxy services push rights holders to make a request for disclosure of registrant data, adding a burden for rights holders. It should be investigated how to balance rights holders' interests in dealing with proxy services and put in place a standardized system allowing immediate disclosure of registrants' information upon request. **FC:** This is important since proxy services can help criminals and delay investigations. A quick and simple procedure should be found, drawing from the Budapest Cybercrime Convention and/or the 24/7 OAS CSIRT. Proxy services could be useful for registrants concerned about privacy or security when legitimate reasons for anonymous speech could justify anonymity. **BC:** Privacy/proxy services may provide a solution for registrants with legitimate concerns about anonymity, but there is ongoing abuse of such services both by providers and registrants, noted in studies as “critical failures”. As registrants pay to protect their information using a proxy service, both the registrant and the proxy service reap a benefit and both must also adhere to the WHOIS requirement. A registrar’s “proxy service” may also simply be a shell to shield the registrar’s own cybersquatting and other illegal activities. ICANN should create guidelines and best practices for privacy/proxy services and step up compliance audits of such services. A study should provide data on the nature of registrants using privacy/proxy services. The findings of this study will provide understanding of the entities and activities of registrants using privacy/proxy services. The findings will set a baseline for evaluating policy changes indicated by other WHOIS studies.
6. How effective are ICANN’s current WHOIS related compliance activities?	**VH:** ICANN's activities to keep the WHOIS data accurate did prompt our registrar to take action, otherwise the domain might have been lost. Mailing the registrars in order to check the WHOIS data is a good practice. **MN:** They are open to abuse. Many WHOIS complaints are more about disputes between 3rd parties than about compliance. **IHG:** Some registrars make little effort to comply with WHOIS requirements. This enables malicious registrants to engage in infringement,

	to the benefit of those registrars, while undermining the efforts of ICANN to maintain open access to data. Without consequences of WHOIS non-compliance for registries and registrants alike, inaccuracy will pervade the WHOIS database. *See submission for example.* **INTA:** ICANN's Whois related compliance activities are ineffective, as ICANN lacks tools or resources to be effective. Despite the rollout of new gTLDs, ICANN plans to increase its compliance staff only nominally. A key weakness is the absence of a mechanism to ensure that Whois records are accurate. **IACC:** Recent compliance efforts show improvement but remain insufficient. ICANN's studies show widespread WHOIS non-compliance and ICANN's measurements are unduly forgiving. All studies measure system-wide compliance and understate the extent of the problem with those engaging in illegal activity. ICANN is taking steps to insure compliance with the RAA, but RAA deficiencies hamper these efforts. There has been no effort to enforce registrant compliance so efficacy of this compliance activity remains untested. **TWI:** Key RAA provisions related to Whois data are weak, ambiguous or both. This inhibits ICANN's compliance efforts. ICANN's compliance staff should be more aggressive in pursuing non-compliance with the RAA and bolder in issuing interpretations of the RAA provisions. However, there is a limit to what can be achieved under the current RAA, so ICANN should accelerate efforts to revise it. ICANN could also more effectively enforce compliance with 21 registries than with 900 registrars. 19 of the 21 registries today operate a "thick Whois" in which the public may get full registrant data. The two outliers are the largest registries where public access to Whois (through registrars) is inconsistent and sometimes unavailable. The thin registry model was created in order to stimulate competition in registration services. With that market achieved, ICANN should convert the two outliers to thick registries. Compliance with Whois policies will benefit from that. **CNNIC:** The practice and performance of applying ICANN's WHOIS policies has not met the criteria defined in these policies. WHOIS accuracy of .com and .net has been poor and ICANN has failed to regulate them to maintain accurate WHOIS data. ICANN has neither been effective at developing WHOIS policies nor at regulating registrars to improve WHOIS accuracy. **NOM:** For.uk: In case of incorrect WHOIS data, we put the registrant under notice to correct it and suspend the domain name should this not happen. In specific circumstances - where a law enforcement agency has identified criminal activity under the domain name - we can use our terms and conditions to suspend the domain name. The registrant can appeal against this suspension. **COA:** ICANN should do a better job of enforcing the Whois obligations in its contracts with registrars and registries. Revision of those contracts is needed to provide clearer obligations, also extended to resellers. Current Whois-related RAA provisions are ambiguous, weak, or both. ICANN's compliance capability has improved but far from achieving the necessary "culture of compliance", which requires both resources and re-orientation. With new gTLDs, the contractual compliance burden will increase dramatically, while compliance with current contracts is not yet achieved. One third of the budget surplus from new gTLDs should be devoted to contract compliance and enforcement functions. ICANN should be more proactive in its compliance activities and respond more forcefully to complaints. We commend the compliance staff for deciding to review the WDPRS, which is plagued with problems. We hope this will result in a system that is more receptive to complaints, can handle higher volumes, monitors registrar compliance in investigating complaints, requires registrars to reject unverified corrections and encourages registrars to cancelling domains associated with uncorrected false Whois data. **IPC:** The NORC study showed that only 23% of gTLD registrations is fully compliant with accuracy requirements and that current compliance activities are inadequate to fulfill ICANN's AOC commitment. ICANN's compliance function has made progress, but a change in approach is needed in light of the addition of new gTLDs. **PK:** Not very effective. Some registrars follow up with registrants and get updates when the domain is flagged, other registrars don't care if data is correct and don't seem to care about the obligations. When I get a notice 45 days after reporting a domain and click on the "the

	information hasn't been corrected" link, I see no follow-up action taken by ICANN to attempt to get the information corrected. **HL:** The NORC study found that only 23% of gTLD registrations were fully compliant with accuracy requirements, making it clear that ICANN needs to beef up its compliance efforts. This seems to be happening if one looks at the statistics found on the ICANN Dashboard. From 2009 there was an increase in terms of enforcement with 23 registrars having their accreditations terminated or not renewed. The reasons for registrar loss of accreditation over the last four years often include WHOIS related issues. The falling number of registrars who lost their accreditation in 2010 (13) and 2011 to date (4) could be viewed as a positive indication as more and more registrars ensure that they are compliant with the RAA. However, the decline could also be due to a downturn in the ICANN Compliance Team's activities. It could be useful with an analysis of auditing activities resulting in various notifications cross referenced with actions taken by registrars. **FC:** The RAA should be revised so actors without a direct contract with ICANN can be held liable for misuse of WHOIS. **BC:** ICANN has launched additional compliance activities, including audit of Port 43 access by registrars and an inquiry into reminders to registrants regarding their WHOIS data, but these activities are just the tip of the iceberg in terms of needed compliance. ICANN's own studies show that only 23% of records are fully accurate. An organization with a 23% data accuracy record would be considered failing. Compliance resources are needed to fix this and the issue of WHOIS accuracy becomes more urgent with the rollout of new gTLDs. ICANN's compliance organization is well aware of continuing frauds and abuses. As part of the AoC, ICANN's performance in compliance should be measured to assess whether it is meeting its commitments. **ALAC:** The time has come for a change in the philosophical approach to WHOIS compliance. It has become an article of faith that ICANN Compliance is responsible for WHOIS data accuracy. There is also widespread acceptance that the registry/registrar community is responsible for data accuracy and availability. The low expectations of registrants in this area are often noted. Seeing the complexity of the issues we reject these views as unilateral and simplistic. Compliance needs a balanced approach, given the three sets of actors – registrants, registrars and ICANN Compliance. WHOIS data accuracy is a cost/value proposition with differing perspectives from registrants, registrars and users of WHOIS. 100% accuracy is laudable as an objective, but may be unobtainable and puts an unfair burden on one set of actors in the WHOIS triangle. This objective creates an insurmountable threshold for ICANN Compliance, even with best efforts and more resources available. The public interest may be better served by recognizing that the risks from bad actors tend to be cyclical – higher following the establishment of new domains and decreasing thereafter. There is no rational for the same risk to be ascribed to all domains; domains used primarily for support of business transactions on the Web run a higher risk of fraudulent activities than those used for personal or informational pursuits. Adjustments in compliance approach and expectations of the impact might benefit from a change in the philosophical construct of compliance and the processes used to affect the assurance of compliance.
7. <u>Are there any aspects of ICANN's WHOIS commitments that are not currently enforceable?</u>	**VH:** Item 2, that users can determine if a domain is available is useful, and many services look for free domains by checking WHOIS data, but when enough requests for a domain are submitted, those services register the domain on their own. ICANN should find a way to prevent such practices. Item 6, about user confidence in the Internet, cannot be "enforced" and most users are not even aware of the WHOIS service. Item 7, about the assistance of business and organizations, is not enforceable when a proxy service is used. **INTA:** Accuracy is one area of particular concern as noted in the response to question 6 above. **TWI:** See answer under 6 above. **CNNIC:** According to ICANN's current WHOIS policy, complete and accurate WHOIS information of registrants should be made available to the public. However, it is impossible for ICANN to fully execute the policies. Current policies have not clearly defined registrars' obligations to reach a certain WHOIS accuracy level and the policies conflict with privacy laws in some countries. ICANN should respect and consider

	privacy laws of different countries when developing WHOIS policies, and also more effectively regulate accredited registrars. **COA:** See answer under 6 above. **IPC:** Steps have been taken to resolve issues related to privacy laws. The biggest barrier to enforcement of ICANN's WHOIS commitments is the lack of consequences for the parties involved when accurate and complete WHOIS information is not maintained. ICANN's commitments cannot be met if no negative consequences result for ICANN, registrars, registries or registrants who supply false data. Lack of due consequences gives the appearance that the commitments are unenforceable. **PK:** ICANN must be willing to cancel its agreement with a registrar if the registrar fails to comply with the terms. The biggest example of this is the misuse by DROA, using WHOIS as their mailing list, with false "renewal notices". ICANN should canceled the agreement with DROA! **HL:** There is a disconnect between compliance with the EU data protection directive and the registrar's WHOIS obligations in the RAA. The Procedure for Handling WHOIS conflicts with Privacy Law seems to address this and it would be interesting to get an overview of how well this is working or if it is indeed open to abuse from "bad actors". **BC:** See response to Question 1. ICANN cannot meet its AoC commitments unless all stakeholders, including registrars, are required to ensure WHOIS accuracy. The RAA should be amended to require contracted parties to verify WHOIS data accuracy and penalties are needed to ensure compliance with WHOIS obligations related to accuracy and access. ICANN manages registries and registrars through contracts, so anything that can be made part of those contracts should be enforceable. That includes new consensus policies adopted by ICANN that automatically become enforceable on contract parties. Given this, all ICANN's WHOIS commitments can be made enforceable.
8. <u>What should ICANN do to ensure its WHOIS commitments are effectively enforced?</u>	**VH:** Promote and explain the WHOIS service to normal users. **IHG:** Compliance with WHOIS data reporting should remain compulsory and included in the RAA. Noncompliance should be met with enforcement, including fines. Registrants who submit false information should have all their registrations suspended until WHOIS data is correct. Severe repercussions should be reserved for registrars who intentionally disregard WHOIS policy, and profit from illegal and unethical registrations. With no disincentive to non-compliance with WHOIS requirements, registry services have little motivation to publish registrant data that could be accessed by competing registries. This could lead to hoarding of registrant data by registrars to prevent rivals from obtaining a competitive advantage. If WHOIS requirements are fully enforced, some mechanism is needed to prevent this scenario and quell registry reluctance to publish client data. **INTA:** Include clear obligations in the registry and registrar contracts and provide clear advisories on those obligations if differing interpretations emerge. Significant resources are needed to monitor compliance and ensure that effective enforcement is in place. Another option is to implement thick Whois at the registry level in order to have a single validation point. The provision of Whois information at the registry level under the thick Whois model was deemed essential by the IRT and advanced as one of their five key recommendations. **IACC:** ICANN must amend the RAA to reflect the interest of the wider community, not only the registrars. The amendments should clarify ICANN's and registrars' responsibilities for a transparent and accurate WHOIS and should provide meaningful tools for ICANN in the event of noncompliance. ICANN should commit more resources to compliance and deploy those resources to increase WHOIS accuracy. **TWI:** See answer under 6 above. **COA:** See answer under 6 above. **IPC:** A change in enforcement policy is needed. Policies need to be developed which provide incentives for compliance by registrars and consequences for both registrars and registrants when WHOIS information is not available in line with the AOC commitments. **PK:** Cancel the agreement with DROA and take action when necessary. Don't be like the government and create rules if you're not willing to

	enforce those rules and stand up to those who would take advantage of your inaction. **HL:** The AoC requires ICANN to maintain timely, unrestricted and public access to accurate and complete WHOIS data – and enforce this. ICANN should ensure that WHOIS accuracy is a requirement with clear consequences for failure to comply by either registrar or registrant. ICANN needs to continue auditing registrars to ensure RAA compliance and to weed out non-compliant registrars who don't cure when alerted. The removal of "bad actors" is essential to provide assurance to the community. By placing the registrars under pressure with the threat of loss of accreditation, ICANN is correctly focusing its compliance efforts. The WDRP could be made more robust by stating that failure by the registrant to confirm WHOIS data would be grounds for the cancellation of a domain. **FC:** Warnings and then fines. In civil law it is commonly used when gathering personal data to assure that they are correct to sign affidavits. To provide incorrect information is a felony. **BC:** See responses to Questions 1, 5 and 6.
9. <u>Does ICANN need any additional power and/or resources to effectively enforce its existing WHOIS commitments?</u>	**VH:** I don't think so. **IHG:** The compliance task is monumental and additional compliance staff and budget will be needed to achieve complete and accurate WHOIS data. ICANN should devote one-third of the surplus revenue from new gTLD applications to contract compliance activities. **INTA:** In light of the addition of new gTLDs, the compliance department must be expanded significantly in both staff and authority to ensure enforcement of existing Whois commitments. Accreditation of privacy/proxy services would go a long way to promote compliance. **IACC:** Yes. Better tools should be provided through the RAA and ICANN should allocate resources to insure compliance with WHOIS requirements by both registrars and registrants. **TWI:** See answer under 6 above. **COA:** See answer under 6 above. **IPC:** Resources are critical and one-third of the surplus revenue from new gTLD applications should be dedicated to contract compliance activities. ICANN's compliance philosophy needs re-orientation. ICANN has stepped up its compliance efforts, but still approaches the commitment as one that may be impossible to accomplish. Compliance staff has stated that many registrars "don't know their obligations" for WHOIS and that it is unclear who is responsible to comply with the RAA provisions. Policies are needed that require registrars to take proactive steps to institute WHOIS compliance programs. Registrars should designate a WHOIS Compliance Officer responsible for WHOIS compliance. That officer should list contact information with ICANN's compliance department and failure to keep that information current should have consequences. Registrants should bear consequences including freezing and cancellation of the registration; and ICANN compliance staff should aggressively monitor registrar actions to ensure these consequences occur. ICANN should publish ratings of registrars based on WHOIS accessibility and quality, and efficiency in combating false data, to inform the public. **PK:** Additional resources? Maybe. Additional power? No. ICANN already has all the power it needs to pull the plug on registrars and registrants that are not willing to comply with long established rules for domain ownership. **HL:** Registrar and registry compliance is of growing importance and ICANN must show that it is taking this issue seriously. ICANN should also demonstrate that it has sufficient resources to enforce compliance of the agreements with the registrars and potential new gTLD registries. By doing so, ICANN will reassure the community that registrars (non)compliance with the RAA is being addressed seriously. Compliance and associated issues will increase with the new gTLDs and the issue of registry/registrar vertical integration and full cross-ownership. ICANN will require significantly more resources for compliance issues. In June 2010, the then Senior Director of Contractual Compliance, David Giza, stated that there were six people working in compliance within ICANN, that they were understaffed and

	underfunded. and that they only had one auditor, needing at least six in order to address the compliance issues. Staff lists show that there are eight people involved in compliance and this needs to be improved upon. With new gTLDs, compliance issues will increase overall. Funds from new gTLD applications need to be used to beef up compliance in proportion to the number of new gTLDs accepted. The funding of compliance activities has been lacking for years, and is the reason why many registrars have no concern about such issues.
10. <u>How can ICANN improve the accuracy of WHOIS data?</u>	**VH:** Provide a service for registrants to update their data directly on an ICANN website. The intermediate step with a registrar often fails since some don't update the information. Remove all prices for domain updates. Updating a domain should be free. **MN:** Give private registrants the ability to "opt out". **IHG:** Shifting some or all responsibility of maintaining data to the registrant could make WHOIS more dependable. Registrars have little ability to confirm that data provided by registrants is reliable, making it problematic to charge those with ensuring data accuracy. A RAA provision for compulsory data authentication would provide registries with the ability to comply with WHOIS reporting requirements. **INTA:** There are no mechanisms in place to ensure the accuracy of Whois data provided by registrants, just a presumption by registries and registrars that such data provided by registrants is accurate and a lack of incentives for registrants to provide accurate data. A validation process funded by additional fees paid by registrants should be considered, as well as penalties like loss of registration if data is found to be inaccurate. In cases where Whois data problems have been reported, there should be obligations to verify any replacement data offered by the registrant, as opposed to applying the same presumption of validity once any change has been made to the inaccurate data. **IACC:** Amendment of the RAA, enforcement of its WHOIS provisions against both registrars and registrants and publication of policies to the community to inform about these changes. **TWI:** Inaccurate Whois data is a problem that undermines the goals of the service, erodes public confidence in the online environment, complicates online enforcement of consumer protection, intellectual property, and other laws, and increases the costs of online transactions. ICANN has taken steps to quantify the scope of this problem but has done little to address it. The RAA puts responsibility for Whois data accuracy on a party with whom ICANN has no contractual relationship – the registrant. Registrars have the obligation to investigate reports of false Whois data, but no responsibility to check the accuracy of the data submitted, nor an obligation to cancel the registrations of those who submit false data. The responsibility for Whois data accuracy must be shifted to those that can achieve it and have contractual obligations to ICANN – registrars, registries or both. ICANN has taken steps toward this goal in the gTLD environment. In three registry agreements (.mobi, .tel and .asia) there are Whois data quality obligations that flow through registries to registrars. ICANN was asked to do the same for all new gTLDs, but refused. However, ICANN has given an advantage to new gTLDs that verify registrant data by giving them an extra point in the evaluation. Whois accuracy Improvement may occur once these practices become norm for new gTLDs. **NCUC:** See answer under 4 above. **CW:** Accuracy of the data has always been requested. If nearly 30% of records are still inaccurate, we might be barking up the wrong tree. Registrars have long asserted that full verification of the accuracy of all records, including a considerable backlog, would be financially unsustainable. If so, a different approach is needed. If not, then serious compliance efforts would be required, including budgetary aspects. As this matter has not been resolved since the creation of ICANN, I wonder what new elements have arisen to facilitate a solution now. **MPAA:** See answer under 1 above. **NOM:** For.uk: We have assessed the accuracy of .uk WHOIS and found that accuracy of opted-out domain names is higher than average, with 92 % traceable postal addresses. We perform overviews by batches. **COA:** Current high levels of inaccurate Whois data flow from ICANN's decision to place sole responsibility for Whois data quality on the

	registrant with whom it has no contractual relationship. Registrars insist that their only contractual obligation is to respond to reports of false Whois data, rather than to verify data accuracy or cancel registrations based on false Whois data. The largest registries have even less role to play on Whois data quality currently. Registries and registrars should share responsibility for Whois data quality, with greater involvement of registries through "thick Whois", which all but two gTLD registries now employ. In these gTLDs with registrant data maintained by the registry operator, as well as on a distributed basis by registrars, the registries share responsibility for Whois accuracy (and availability), and provide a more accessible and accurate Whois. While there may be technical issues in transitioning .com and .net to thick registry operation, ICANN should commit to doing so and set a timetable for achieving this. There should be "Flow through" obligations to registrars. Registries in three gTLD registries (.asia, .mobi and .post) are required to hold their registrars to Whois data quality standards. ICANN should revise all registry agreements to incorporate similar standards. There should be data verification requirements when registrar collects registrant data. Currently, registrars reject any contractual obligation to ensure that data is complete and accurate. Registrars can do much to check and verify the data the registrant presents and they do check for billing information (credit card data), but not for Whois data. ICANN has never required them to take these steps, but has made it clear for new gTLDs that verification of Whois data is preferred, giving an extra point to new gTLD applicants with such a commitment. Not until this approach is made the norm will significant progress toward more accurate Whois data be achieved. **IPC:** Policies are needed that provide for proactive registrar compliance and for consequences associated with inaccurate data. ICANN should swiftly bring the last two gTLD registry outliers (.com and .net) to operate thick Whois; require all gTLD registries to pass on to their registrars Whois data quality obligations, building on provisions in the .asia, .mobi, and .post agreements; and operationalize the preference expressed in the new gTLD evaluation criteria by providing all gTLD registries and registrars with incentives to verify Whois data. **PK:** By enforcing current regulations and canceling agreements with registrars that fail to comply with obligations. Registrars should be reminded that they should cancel registrations for registrants that don't provide accurate and complete data. **HL:** By continuing to focus on registrar compliance with their WHOIS obligations, ICANN can take steps to ensure accurate WHOIS data. Enforcement of section 3.7.7.2 of the RAA with threat of termination of the accreditation if appropriate action is not taken provides good leverage to ensure accurate WHOIS data. The citation of this section has often resulted in action by the registrar to contact the registrant and to ensure correct WHOIS data. Trade mark owners should not have to pay legal counsel to cite this section in order to clean up WHOIS! The WDRP could be made more robust by stating that failure by the registrant to confirm WHOIS data would be grounds for cancellation of a domain. For new and existing gTLDs there should be incentives for registrars to verify WHOIS data, since they verify the billing data. **FC:** The registrar has to take into account the purpose and quantity limitation when gathering data, then find a way to prove that the information is accurate by asking for proof of the information given such as a phone bill. **BC:** See responses to Questions 1, 2, 5 and 6. **CIRA:** ICANN can adopt measures to enforce compliance with accuracy requirements. In designing any measures, ICANN should consider the factors that lead to inaccurate and incomplete WHOIS data. Solutions can include registration validation; keeping in mind that the solution must be practical. Any validation program requires significant verification, maintenance, and a compliance system, duties which must considered in the design. In addition, registrants who provide false data should not benefit from privacy/proxy services.
11. <u>What lessons can be learned from approaches taken by ccTLDs to the accuracy of WHOIS</u>	**VH:** I am not aware of the approaches taken by ccTLDs. **SIDN:** SIDN is not subject to any obligation to provide any whois service on the .nl-domain at all. We do however provide such services, historically because everyone did it and currently because it is in the interest of our local internet community. Whois has been the subject

data?	of extensive discussions. Until 12 January 2010 SIDN offered a full and open whois, comparable to the gTLD's, but changed that after the last consultation with stakeholders to better protect the privacy of the users. Also in the Netherlands Whois discussions are always ongoing and what is there today might not be there tomorrow. A number of 'solutions' that we use are not exactly scalable to gTLD's. We use the fact that we are a country code TLD and for example only provide non-public whois details to Dutch law enforcement agencies and to Dutch based attorneys. We have never received any approval (nor disapproval) from the Dutch Privacy Authority with regard to our current Whois services. So do not automatically assume that what we do is completely in line with the Dutch and/or European privacy laws. **AFNIC:** In addition to the data publication and access policy, AFNIC has always been involved in enhancing whois data accuracy. Our current policy is summarized in Art. 16 of the .fr Charter. AFNIC conducts two types of accuracy checks. For companies and legal organisations, AFNIC checks public databases to ensure that data is accurate. These checks are performed no later than 30 days after registration. 10 to 20 000 checks of this kind are performed each month, with some automation. For private registrants, checks are performed on request and involve registrars checking accuracy. In 2010, AFNIC performed 386 checks of this kind. By virtue of French law, providing inaccurate data may lead to cancellation of the registration. This may only happen after the registry has offered the registrant a chance to correct the data. **INTA:** By placing a priority on contractual compliance, registries can improve the integrity of Whois data within their TLD. **IACC:** Some ccTLDs (e.g. CCNIC) have WHOIS data verification that may be appropriate to examine. Verification of registrant data combined with action to delete non-compliant domains should be considered as a compliance tool. ccTLDs for countries with domestic privacy laws have experience balancing data privacy restrictions with the need to provide accurate WHOIS data to law enforcement and civil litigants. Some ccTLDs have implemented thick WHOIS at the registry level, and may provide insight into whether such systems lead to more accurate WHOIS data. **TWI:** See answer under 3 above. **CNCERT:** With the development of the Internet, cybercrime causes losses to governments, enterprises and users. Registrants can be looked up in WHOIS, but the real users of malicious domains provide fake information to escape from investigation. In the long run, inaccuracy of WHOIS data is detrimental to the development of the Internet. The Review Team can benefit from worldwide experience and push ICANN to establish guidelines to increase WHOIS accuracy. China has strengthened verification of WHOIS authenticity and accuracy of .CN and it is very effective. Malicious domains and phishing sites have almost disappeared, although malicious users abandoning .CN domains continue to commit crimes through other TLDs. CNCERT/CC has processed domain abuse through regional platforms such as FIRST and APCERT, but the coverage of those organizations is limited. CNCERT/CC hopes that the Review Team can consider those methods in gTLDs. International coordination including most of the registries and registrars need to be established to handle domain name abuse more efficiently. **CNNIC:** In 2009 and 2010, CNNIC started to improve WHOIS accuracy by verifying registrants' data. By the end of 2010, WHOIS accuracy has reached 97% and domain name abuses plummeted to a negligible level. The most important lesson is that collaboration with registrars is key to improve WHOIS accuracy. The current policy is that registrars are asked to collect real WHOIS information from applicants, and failing to do so may imply de-accreditation. With the help of our registrars, the WHOIS accuracy of .cn has been fundamentally improved. **NOM:** ccTLDs are focused on serving the needs of specific jurisdictions, which allows them to tailor their approach to local circumstances. Privacy is an issue and ignoring it will increase the probability that data will be incorrect, even from those without malicious intent. In the case of.uk, Nominet has a contract with the registrant and can use this to require corrections. However, data may be incorrect due to misunderstandings, not updated when circumstances change or changes may not be passed on to our systems. We work on improving data quality by proactive checks and in response to complaints, and act quickly when malicious activity is suspected. This remains our priority.

	IPC: Accuracy of WHOIS data is also important for ccTLDs and many have undertaken WHOIS accuracy studies, such as Nominet and CIRA. As to actions to improve WHOIS accuracy, a prime example is CNNICs approach. In 2010 CNNIC sent out emails to the registrants of .CN requesting that they verify that their data was correct. Registrants could confirm details by clicking on a link in the email. Recipients had 15 days to respond and absent confirmation by the deadline, the domain ran the risk of being deleted. Some aspects of the CNNIC approach seem problematic, including the short deadline and the requirement to click on a link in an e-mail, a practice to avoid for security reasons, but placing the onus on registrants to confirm Whois data accuracy is worth pursuing. ICANN may consider requiring an e-mail to be sent to registrants to which they must reply, within a reasonable time limit, to confirm the accuracy of their Whois data. Alternatives might be to have registrars require users to log into their accounts and click on a box. Such an approach goes a step beyond the current WDRP and may be more effective in improving Whois accuracy. Also see answer to question 3 above. **PK:** How good are ccTLDs at enforcing their registrar's commitments? And what impact does that have on WHOIS accuracy? **HL:** Accuracy of WHOIS data is also important for ccTLDs and many have undertaken WHOIS accuracy studies, such as Nominet and CIRA. As to actions to improve WHOIS accuracy, the prime example is CNNICs approach. In 2010 CNNIC sent out emails to the registrants of .CN requesting that they verify that their data was correct. Registrants could confirm details by clicking on a link in the email. Recipients had 15 days to respond and absent confirmation by the deadline, the domain ran the risk of being deleted. This approach was criticized as CNNIC did not give any prior warning and registrants had no time to prepare. Owners of big domain name portfolios with many Chinese domains were concerned about responding for each by the deadline. However, ICANN may wish to consider 1) placing the onus on individual registrants ; 2) incorporating elements of this approach in a review of the WDRP, with notice and a longer deadline (circa 3 months); 3) requiring an e-mail to be sent to registrants to which they must reply, within a reasonable time limit, to confirm accuracy of their Whois data; 4) reviewing the various ccTLD WHOIS accuracy studies and approaches to consider whether any could be applied to gTLDs. **BC:** A ccTLD aspect to consider is whether accuracy is improved by a “thick” WHOIS data maintained at the registry level. **CIRA:** Addressing WHOIS accuracy and completeness requires much work. The longer it is left unaddressed, the worse the problem will become and the harder it will be to implement solutions as the volume of inaccurate WHOIS data will grow. WHOIS accuracy and completeness is important to CIRA as we have eligibility requirements (Canadian presence) for registrants. Revoking registration due to incorrect data is one method of ensuring accuracy and completeness.
12. <u>Are there barriers, cost or otherwise, to compliance with WHOIS policy?</u>	**VH:** Costs! Many hosting providers do not update WHOIS entries. **MN:** Validation of registrant data is costly. Registrars rely on the data received as provided in good faith. It may be possible to validate some input, such as an email address, but it is financially prohibitive to attempt to validate all registrant data. **INTA:** Aside from costs, there are no barriers to compliance with Whois policy. The costs of not maintaining accurate Whois far outweighs the cost of compliance and should be shared by registrants, registries and registrars alike. **TWI:** See answer under 6 above. **NCUC:** Even with the policy for resolving conflicts with national law in place, WHOIS poses problems for registrars in countries with differing data protection laws. Registrars do not want to wait for an enforcement action before resolving conflicts and many data protection authorities will not give opinions without a case. ICANN's response that there's no problem does not suit a multi-jurisdictional Internet. **CNNIC:** Verifying WHOIS data implies extra costs for registries and registrars. In addition, registrants, especially in .com and .net, are used to submit inaccurate WHOIS data, due to lack of obligation and verification. The cost of verifying WHOIS data and educating registrants are the biggest two obstacles to compliance with ICANN WHOIS policy.

	NOM: A main barrier is in the processes that link registrar and registry data systems. We work with registrars to improve these processes. **COA:** See answer under 6 above. **IPC:** The biggest barrier is failure to make WHOIS data a real priority. The costs incurred by registrars or registries to comply with Whois requirements are the costs of doing business in a responsible way that enhances consumer trust and meets public interest. If enforced even-handedly for all, any competitive impact of increased costs should be minimal. **PK:** ICANN's unwillingness to take action against registrars that don't take action with their non-compliant domain holders. **HL:** Cost-related barriers to compliance with WHOIS policy should not be a consideration for ICANN. Registrar and registry WHOIS compliance ise of prime importance. The task of auditing and policing registrars may be daunting, but ICANN must take it on to avoid a loss of faith in its ability to manage the situation and deal with new gTLDs. **FC:** Full and deep understanding of WHOIS Policy might be one. **BC:** A barrier to WHOIS compliance is lack of management attention to RAA enforcement. Lack of fact-based data on WHOIS and privacy/proxy registrations is a barrier to policy development, but studies underway should provide results. A significant barrier to improving WHOIS will arise if contracted parties block new policy development processes and contract amendments.
13. <u>What are the consequences or impacts of non-compliance with WHOIS policy?</u>	**VH:** WHOIS entries are no longer seen as a reliable source of information. **IHG:** Non-compliance with WHOIS policy reduces data reliability, burdens brand holders with protectionist activities, and detracts from user confidence in ICANN and the Internet. With the increase of new gTLDs, WHOIS compliance should be a priority and policies be developed to include accountability and enforcement measures prior to the award of any new gTLDs. **INTA:** Crime and fraud are key motivators for provision of inaccurate Whois data and use of privacy/proxy services. They are the logical outgrowth of non-compliance with Whois policy. **IACC:** Inaccurate WHOIS has a negative impact on stability of the Internet and on our members' ability to enforce IP rights. Experience with WHOIS since ICANN assumed custody has shown that unscrupulous Internet users are among the first to disregard their obligations to provide accurate WHOIS contact data. Online counterfeiting has been aided by ICANN's failure to administer the WHOIS system as stated in agreements including the AOC. Ineffective WHOIS compliance is not the only cause of online counterfeiting, but the extent is caused by the ease with which online pirates can disregard WHOIS by providing false data and, when found out, change to equally invalid contact data. **TWI:** See answer under 6 above. **NOM:** A domain can be suspended or cancelled if a registrant does not comply or does not correct data in response to a request. **COA:** See answer under 6 above. **IPC:** There are virtually no such consequences, since registrants, registrars or registries that do not comply face no penalties. The result will be increased complaints from consumers and rights holders, pressure for national legislation and an erosion of consumer trust. With unlimited gTLDs, consumer safety and fraud issues will increase when unethical registrants continue to escape enforcement. Inaccurate WHOIS data contributes to public mistrust and instability. When ICANN's approach to its AOC WHOIS commitments is judged insufficient, governments may legislate for WHOIS compliance based on concerns expressed in the GAC Principles. WHOIS compliance should have top priority and ICANN needs policies with accountability and enforcement measures prior to signing new gTLD contracts. **PK:** It makes it difficult or impossible to contact owners of compromised servers with phishing sites. The same difficulty exists when trying to contact people whose servers are used for spam. Many are frustrated by the lack of consistent and accurate WHOIS data. **HL:** There are far reaching consequences of registrar and registry non-compliance with WHOIS policy. As outlined in the GAC Principles,

	WHOIS services are used to assist LEAs, to assist trade mark and copyright enforcement and to combat fraud. Reliable and accurate WHOIS data contributes to end user confidence, encourages use and promotes good faith interactions. If WHOIS cannot be relied upon, the Internet may become the wild west where criminals and fraudsters can operate with impunity. Such a situation would be a huge loss of faith for the end users and is unacceptable for the whole community. ICANN must invest substantial resources in compliance. **FC:** Consumer trust in ICANN or the Internet decreases, impacting ICANN credibility and organizational strength negatively. **BC:** Noncompliance with WHOIS policy has a deleterious effect on ICANN's mission and its ability to meet its AoC commitments. Inaccurate and false WHOIS negatively impacts the Internet's security and stability, impairs the ability of consumers to understand the source of legitimate products/services, facilitates fraud, impairs law and IP enforcement investigations, and harms e-commerce. Problems with WHOIS combined with non-compliance lead to loss of confidence after the introduction of new gTLDs. A full review of the WHOIS system should be made and prompt implementation of recommendations from that review, preferably before the rollout of any new gTLDs.
14. <u>Are there any other relevant issues that the review team should be aware of? Please provide details.</u>	**VH:** Some providers don't update WHOIS. The community should be involved in developing the WHOIS service and protocol. **IHG:** The business community shield their brands and customers from cybersquatters' operations through defensive registrations in the thousands. In capital constriction times, these portfolios become cumbersome and detract from funds to engage cybersquatters via the dispute resolution process. Attempts to scale back defensive registrations are met by increased cybersquatting. The problems associated with inaccurate WHOIS data is a greater problem today than at any time in the past. **INTA:** The Committee has not identified additional issues for the review team at this time. **NCUC:** Permit a registrant to get a domain showing no WHOIS information at all, with the risk that the domain will cease to resolve if the domain is challenged and the registrant is unresponsive. This is the de facto situation for domains registered with false data, so make it an official option. Proposals for verification of information are unworkable for standard gTLDs, but might be launched by registries trying to differentiate. There is no standard of physical addressing that holds across geographies and cultures. Inaccurate WHOIS data should not be used as evidence of bad faith, especially in the context of ICANN's policies such as the UDRP. Within the UDRP, the need to identify a registrant is vital, but WHOIS details should not be used to make determinations concerning abusive registrations of domain names. **CW:** Who does "the public" refer to? Few members of the general public are interested in registration records, which is quite understandable. The interested parties are law enforcement and the IP community. It would be preferable to be specific and seek legally safe and workable solutions to their legitimate needs, which are not necessarily the same. In view of the large number of registrations said to be inaccurate, domains engaged in fraud would tend to be among them. **NOM:** There is a trust issue associated with inaccurate contact data, in particular for domains used for trade. This creates a question of trust for the TLD in relation to law enforcement, regulatory and other public authorities. This could impact consumer confidence, but very few users are aware of WHOIS. The EU's e-Commerce Directive has requirements for trading websites to include contact information so that third parties know who they are dealing with. For the consumer, this information is more accessible than WHOIS. Nominet has a one-stop shop portal for information and links and contributes to awareness initiatives as WHOIS data can be abused to assist fraud and spam. **COA:** The gTLD Whois database is a vital public resource and ICANN's stewardship of it has been ineffective. The proliferation of proxy registration services has contributed to Whois data inaccuracy. Reform is needed, beginning with ICANN enforcement of standards for proxy services. Registries and registrars must assume responsibility for accurate Whois data, through adoption of thick Whois models for all gTLDs; data accuracy obligations that flow from registries to registrars; and verification of registrant data. ICANN's compliance activities need more resources and a proactive reorientation. The AoC spells out the task of the Review Team, but another way is to evaluate how

	effective ICANN has been as steward of the Whois database. Whois is crucial for accountability and transparency on the Internet. When ICANN was established, the gTLD Whois was unified, accessible 24/7 and fully searchable, but had problems of inaccuracy. After a dozen years of ICANN stewardship, Whois is fragmented, has limited searchability and remains seriously inaccurate. A new source of inaccuracy flows from the proxy registration services with some 20 million domain names. On ICANN's watch, the value of the Whois database to the public and its role in promoting consumer trust has degraded and its stewardship has been ineffective. Reversing this degradation of Whois is the challenge ICANN must confront. This long-term view is useful for evaluating the questions the Review Team is tasked to address and in preparing recommendations for improvements. **PK:** Just fix the current system. The Review Team should describe the intentions for WHOIS and spell out why the RAA requires WHOIS data to be complete and accurate. The longer ICANN takes to address compliance, the more effort and resources will be needed to achieve it. **HL:** The issue of WHOIS is of prime importance and should be addressed by ICANN compliance. With new gTLDs, these issues need to be considered now and resources allocated to ensure a response to the Whois problems that face the community now and in the future.
Other comments	**LE:** WHOIS contact info is supposed to work for technical problems with a domain and this is typically not the case for e-mail addresses. ICANN should educate the public about WHOIS using the "annual reminders". RFC 3912 failed to cover the administrative parts in RFC 954, and failed to follow the IETF i18n policy in BCP 18 (RFC 2277). The i18n issue can be fixed, but RFC 5198 was published after RFC 3912. RFC 5198 explains how to replace US-ASCII by UTF-8 in protocols such as WHOIS. RFC 1032 covers the lost administrative parts in RFC 954, but it is not state of the art and needs updating. Even an experimental RFC would have more impact on the community than any ICANN PDF. **SL:** The Whois discussion is a phantom-discussion as most administrators are happy with it as is. Phone and fax number should stay optional, while name and postal address are necessary. For a company, a named person is still necessary as well as an email address. Persons who put false data in whois for a domain should lose the right to the domain. **VH:** WHOIS has always been important for data about domains and their registrars but customers don't understand why personal data is published, while others may use proxy services or provide false data on purpose. It is difficult to find reasons why WHOIS still has to contain personal data. Remove personal data from WHOIS but keep WHOIS alive by making it more important for technical questions. **MM:** The following paper with a historical overview of the evolution of Whois could be helpful to the Review Team's work: http://forum.icann.org/lists/whoisrt-discussion-paper/pdfDB3W7kd4BR.pdf **MN:** The RAA provisions are problematic, as they demand registrars to make public whois available, offer bulk whois access to anyone and protect registrants from unsolicited marketing. Those requirements are conflicting and at odds with EU privacy law. There is a process to handle that but it's unclear if it has been used: http://www.icann.org/en/processes/icann-procedure-17jan08.htm **EL:** All gTLD registrars must support WHOIS and have links to their WHOIS servers. Owners of domain names must be kept accountable for their actions. Even though an email address may be obfuscated, there must be some way to contact the registrant. **BS:** Whois is fine for businesses but a problem for personal websites. An individual's alternatives are to release personal information, make whois data private, insert false whois data or pay for a PO box and put that in as whois address detail. None of these choices are ideal. A solution is needed that doesn't involve sacrificing privacy. Give the option to hide the physical address for individuals. The provider should have full access to address info at all times but the public should not. **AFNIC:** AFNIC welcomes the opportunity to provide insights from our experience as ccTLD manager for .FR to questions 3 and 11 of the Discussion Paper. We stress that the framework stems from the French legal environment with legal and regulatory measures enforced by the electronic communications Act, instructions for the French privacy authority CNIL and registry policies, developed in a multistakeholder

	process, as well as AFNIC's commitments towards the French Government. **IHG:** WHOIS helps combat malicious exploitation of trademarks by those who intentionally register domain names that are confusingly similar to those of well-known brands. Cybersquatting continues to evolve, while the means to combat it remain static. Open access to accurate WHOIS data must be reinforced to develop additional brand protection measures as well as promote trust. Inaccurate WHOIS data impedes dispute resolution and compromises the integrity of the registration infrastructure as well as trust in the Internet. **INTA:** Trademarks are a primary means for consumers to make informed choices of products and services. **IACC:** The IACC supports the review of ICANN's compliance with its WHOIS obligations, and trusts the review can increase transparency and stability of the Internet. **TWI:** Whois data is the foundation for most Internet-related investigations and transactions and we rely upon access to this data for starting investigations of rights infringements. We also use it for routine tasks in managing domain portfolios and for domain transactions. Access is also essential to LEAs, consumer protection organizations and users who need to know whom they are dealing with. This data has to be accurate, complete, up-to-date and readily accessible as a crucial Internet resource. The Review Team's role is to evaluate the quality of ICANN's stewardship of this resource and recommend how to improve it. This is the most critical of the reviews mandated by the AoC. **NCUC:** The NCUC is concerned about the lack of adequate privacy protection in WHOIS and believes ICANN can offer better options for registrants and the Internet-using public, consistent with its commitments. **CW:** While commending the Review Team for assisting ICANN to address the Whois issues, it should be noted that these issues have been addressed repeatedly during the past decade, without resolution. The issues remain important, but it is not clear what new elements have emerged since the AoC to create expectations of a successful outcome on this occasion. **MPAA:** Our comments respond to some of the questions posed by the Review Team, based on our experience in combating copyright infringements carried out through the use of domain names. **CNCERT:** CNCERT collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for exchange of information and coordination of actions with International Security Organizations. **CNNIC:** CNNIC offers WHOIS services through a web-based interface implementing RFC3912. By the end of 2010, the WHOIS accuracy of .cn had reached 97% and spam emails sent from .cn URLs had fallen to less than 5% from 15% in 2009. Reported phishing websites under .cn had been reduced from 86.5% to less than 0.6%. All registrants in .cn are required to provide real WHOIS data, and CNNIC is responsible for verifying the data. Registrars are required to verify applicants' WHOIS data, and WHOIS accuracy is used to evaluate registrar performance. **NOM:** Nominet has developed its WHOIS policy and implementation in consultation with stakeholders. Our contribution provides data about the UK environment in response to the request for ccTLD input. We have not responded to questions on the gTLD WHOIS policy. **COA:** COA has been active in a range of ICANN policy development activities, on its own account and as a member of the IPC. Whois policy has been a focus of the ICANN activities of COA and of its predecessor, the Copyright Coalition on Domain Names (CCDN). **IPC:** Our comments are keyed to the questions posed in the Discussion Paper. **PK:** My company has implemented various protocols and networking products over the years and is active in fighting spam and phishing. WHOIS is essential for contacting actors to report hacking or abuse. Those offering privacy services to registrants should only do so if they also take on the responsibility themselves. **HL:** Hogan Lovells is acting for numerous brand owners and Internet players. **BC:** The Business Constituency ("BC") has long supported the need for greater WHOIS accuracy and access to ensure the protection and

	safety of Internet users and to enable brand owners to protect their intellectual property. We support the goals of the WHOIS Review Team to assess the extent to which gTLD WHOIS policy in the space is effective, meets the needs of law enforcement and promotes consumer trust, and its additional assessment of ICANN's performance in this area. **PK(2):** I'm surprised that people put their remarks into PDF and DOC (and DOCX) attachments rather than in the mail, expecting everyone to use external software to review comments. PDFs are universal, but people should not be forced to have Word or some other reader. **CIRA:** CIRA maintains its own WHOIS service and can offer some insight into practices that encourage accuracy and completeness of WHOIS data. CIRA's WHOIS permits queries to the .CA Registry database to determine the availability of .CA domain names or to view the administrative contact and technical data provided by registrants. Data about individual registrants is not publicly displayed in the WHOIS. Information of corporations is displayed by default. In order to contact a registrant whose information is not displayed in the WHOIS, an online Message Delivery form is used. The message is forwarded to the registrant's Administrative Contact email. For specific disputes that a user has not been able to resolve, CIRA may disclose contact information of registrants that is not publicly available, via a Request for Disclosure of Registrant Information. CIRA may provide personal information in response to a search warrant or as otherwise required by applicable law. For Canadian law enforcement agencies and the conduct of certain investigations, CIRA may also disclose contact information of registrants via a Request for Disclosure of Registrant Information for Law Enforcement. **ALAC:** The ALAC welcomes the Discussion Paper but would have liked to see additional papers identifying the problems regarding the current WHOIS definition, utilization and compliance. We endorse the community-specific conversations hosted by the Review Team in Singapore, where ALAC members participated. The most important objective for the Team is to give a perspective and/or recommend a set of policy initiatives or refinements to existing policy that balance the competing interests in the WHOIS ecosystem. The Team should be in a position to identify and define all of the problems regarding WHOIS, prioritize their impact on consumer trust and confidence in the DNS and make an unambiguous recommendation as to need and focus of correctional policy work. While we have concerns about whether the consumer-focused study authorized by Board funding will add any new information, the ALAC supports collection of as complete information as possible on this issue. The Review Team must pronounce its decisions unambiguously, declaring (1) whether WHOIS as originally devised and for the purpose intended is still necessary, (2) whether the WHOIS dataset as originally determined remains fit to its original purpose, and (3) whether the several uses made of both the WHOIS data and processes that have expanded the original intent are useful and in the public interest. We expect recommendations \ as to whether these additional uses of WHOIS are within the terms and intent of the RAA, are to be embraced by the global community and are within the remit of ICANN Compliance. Answers to these questions will allow interpretations as to (1) whether the present WHOIS dataset is good and sufficient to meet these needs and others that might be contemplated, (2) whether the current processes used for WHOIS data compliance are fit for the purpose. The Team may be able to acknowledge the instance of Privacy/Proxy Services and the role they play in the WHOIS ecosystem and recommend a workable solution that acknowledges privacy concerns, including ways that these may be met in a balanced way.