

Summary of Public Comments on the WHOIS Policy Review Team’s Activities & Definitions

This document provides an overview of the public comments¹ received in response to the request for input, issued by the WHOIS Policy Review Teams, which features the [scope of work and roadmap](#), [action plan](#), [outreach plan](#) and working definitions. The comments’ summaries are grouped per topic referenced and listed in order of submission. Responses without such references are summarized under "General Comments". The summary does in no way substitute for the original contributions, which should be consulted for complete information. The number of comments submitted on this paper tallies up to 18. The comments are hyperlinked below for easy access and available at: <http://icann.org/en/public-comment/#whois-rt>

Contributions provided by:

At-Large Advisory Committee	ALAC	Markus Hanauska	MH
Business Constituency	BC	Messaging Anti-Abuse Working Group I & II	MAAWG
Coalition against Unsolicited Commercial Email	CAUCE	Othello	OTH
European Communities Trademark Association + Marques	ECTA+M	Registrar Stakeholder Group	RrSG
Intellectual Property Constituency	IPC	Registries Stakeholder Group	RySG
International Working Group on Data Protection in Telecommunications	IWGDPT	Ronald F. Guilemette I & II	RG
Jeff Chan	JC	Volodya	VOL
Lexinta	LEX	.nz Domain Name Commission	DNC

RECOMMENDATION/CONCLUSION	SUMMARY OF COMMENTS
<u>General Comments</u>	<p>OTH: See http://forum.icann.org/lists/whois-rt/msg00000.html for details on domain transfers issues in both thin and thick registries. The methods available to registrars for obtaining registrant data are unsatisfactory. The only resource available to facilitate transfers is WHOIS, with an insufficient level of data access.</p> <p>MH: WHOIS data is increasingly less valuable due to fake address entries and proxy services. A central registry of domain owners might be useful but does not need to be public. If WHOIS is abolished, the decentralized database of today would still exist, just no longer public. Questions of local law are at stake (e.g. criminal</p>

¹ The public comment period ran from 4 March 2011 to 17 April 2011.

investigations). Registrars could offer a way to contact domain owners without revealing data. By making all WHOIS data private, the quality will improve more than any ICANN attempt to enforce current policies. The majority of domain owners are neither spammers nor criminals, they wish to protect their privacy. Many more would refrain from using fake data if assured that data will be protected and only revealed to a third party when unavoidable.

VOL: Restricting WHOIS access to LEA² would make matters worse. After hiding the data, the problem would remain but nobody would know about it. An alternative would be to keep the data as public as possible and encourage the use of proxy/privacy services which can be mandated to forward the communication to the real WHOIS holder when non-spam comes in.

MAAWG: It should be possible to obtain registration information in a standard form and with a consistent set of parameters, as for thick registries. ICANN should require transition of all registries to a thick WHOIS. MAAWG opposes allowing only LEA access to WHOIS. Many issues are outside the scope of LEA and dealt with by security and systems administration professionals. WHOIS is critical for a safe Internet for end users. WHOIS must be as robust and highly available as the DNS and certain data-points must be available to security-related assessment systems. This should be considered a minimum and ICANN must enforce compliance with the rules. Overuse of proxy services impairs security systems' assessment of incoming data. The WHOIS DPRS should be available to the public under reasonable and nondiscriminatory conditions. ICANN should report quarterly on WDRPS reports received, related registrars and follow-up actions. Technological improvement is needed and MAAWG hopes this will be taken into account (e.g ARIN proposal).

CAUCE: WHOIS is a critical anti-abuse resource and needs to be a true production service offering with consistent formatting in contrast to current practice under thin registries. WHOIS is a community resource and access to it cannot be restricted to LEA without endangering security, stability and trust. WHOIS data must be meaningful but is too often fraudulent. Anonymity options should be eliminated, in particular for corporations. The current WDRPS system should be improved with provisions for bulk reporting of multiple domain names sharing the same inaccuracies and registrar. ICANN should make WDRPS reports public.

JC: Any reform of WHOIS should consider the likelihood of implementation. An anti-fraud requirement would be that domains have working email addresses to use in the event of abuse. Domains failing this should be at risk of suspension. Proposals to require postal addresses, with non-deliverability of a letter considered proof of breach, are absurd.

² LEA: Law Enforcement Agencies.

DNC: Broad definitions ensure an adequate scope of the review. In many cases WHOIS access and information meet the needs of LEA and, if not, their needs should be accommodated rather than changing WHOIS to meet them. The review scope should state that it does not impact or reflect WHOIS policies relating to the ccTLD community.

ECTA+M: The WHOIS RT should bear in mind the role WIPO plays. ECTA+M support the AoC statement: *such existing policy [...] administrative contact information*- see <http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm>.

Attempts to narrow the scope will have detrimental effect; WHOIS is vital in combating internet abuse. ECTA+M support the maintenance and improvement of WHOIS. Abolition is counter to the AoC and would lead to an increase of abusive activity.

RG: The RT and Internet community are struggling with questions about the intended uses of domain name WHOIS service and how the service can be made to fulfill its intended uses. There is no charter that codifies the formally anticipated and accepted uses of WHOIS. Such a charter should be produced and the RT could acknowledge this as a goal. Absent this context, the *Law Enforcement* definition would be superfluous. Constituencies may have divergent views on availability and some may favor exclusive access, but LEA should not be the sole authorized users of WHOIS. WHOIS is a source of information for network abuse researchers seeking correlations or patterns, which is an authorized and intended use of WHOIS. The accuracy of the current WHOIS is abysmal and ICANN has neither means nor interest in doing anything about it. Solving the problem is neither prohibitively complex nor costly even though ICANN and registrars attempt to make it appear so. Name, snail-mail address, phone number and email address are generally available in the WHOIS records, but there is no practical way to validate all. Cost-efficient and automated mechanisms for validating phone numbers (Sedo) should be implemented and costs could be passed on to registrants. Automated validation should be required to complete a registration and performed routinely as an integral part of the registration process. ICANN is in breach of its AoC commitments to implement measures to maintain *accurate and complete WHOIS information* and in breach of its agreement with DoC. This needs to be rectified as soon as possible. There appears to be financial incentives for both ICANN and registrars not to consider content of WHOIS records closely. ICANN should require all registries to make available a WHOIS server that would be open to all with unlimited access and provide the same data currently provided by the thin top-layer WHOIS server for the .COM and .NET., in particular the registration data/time and the current name servers. The RT should consider formally defining registration date/time and requiring a new data field for all WHOIS records (recent registration {payment}, date/time). Anti-spam, anti-malware and anti-crime research would be greatly benefited by an irreversible triple-DES hash of what might be called the payer ID.

IPC: WHOIS policy is among the most important matters addressed by ICANN in its stewardship of the DNS.

ICANN's current policy and implementation are not effective in delivering the *timely, unrestricted and public access to accurate and complete WHOIS information* required by the AoC. A reliable WHOIS database is critical in building public trust in the DNS, e-commerce and Internet. Robust guarantees of WHOIS accessibility and broad definitions of the operative terms in the AOC are essential. There is nothing in the AOC that suggests the existing policy—of open access to WHOIS data that is collected and provided consistent with applicable law—should be restricted merely to conform with a narrow definition of the legitimate needs of law enforcement and the promotion of consumer trust.

ALAC: ALAC welcomes this timely exercise especially given the imminent gTLD program. ICANN's implementation of its WHOIS policy framework is based on the RAA obligations and enforcement mechanisms. ALAC is concerned about ICANN's handling of its obligations to the community for contract compliance and remains underwhelmed by ICANN's inadequate enforcement regime. The RT needs to provide answers on whether the principles espoused by the WHOIS construct in the context of the DNS remain relevant. If relevant, the RT should provide guidance as to whether the mechanisms remain fit to purpose. The content of the WHOIS data set, quality and accessibility are the main concerns. Controversy swirls around the understanding of *timely, restricted and public access to accurate complete WHOIS information* as the basis for mechanisms and processes. Some contend that the WHOIS obligations impinge on registrants' right to privacy and threaten free speech, while some argue that privacy means anonymity and others believe in restricted/mediated access, advocating privacy services and unfettered access to registrant data. ICANN is obliged to ensure the collection of the full dataset as required, to ensure the validity of the contents and to enforce the contract obligations. The "know your customer and provider" rule is necessary to combat fraudulent activities and must be a rule for all transactions with economic implications. Balance must be struck between these contentions and ALAC offers guidelines to forge a workable one – see contribution: <http://forum.icann.org/lists/whois-rt/msg00012.html>. Transparency and accountability demands that registrars remain contractually obliged to collect data to be publicly available and ICANN must hold registrars accountable to this requirement and demand that registrars validate WHOIS data. The right to know should be balanced by a right to know who wants to know.

BC: The BC supports ICANN's effort to review WHOIS policy and advises the RT to focus on: 1) Measures to ensure *timely, unrestricted and public access to accurate and complete WHOIS information*; 2) Penalties for those who fail to provide access to or abuse the above; 3) Development of policy to address abusive registrations that attempt to evade legal process and law enforcement through use of proxy and privacy services. Policy development should be informed by studies now under consideration in GNSO Council (see <http://gns0.icann.org/issues/whois/gns0-whois-pp-abuse-studies-report-05oct10-en.pdf> and <http://gns0.icann.org/issues/whois/whois-pp-relay-reveal-studies-report-11feb11-en.pdf>; 4) Strict enforcement that would require thick WHOIS for all gTLD registries.

	<p>RySG: The WHOIS RT is a key component to meet the specific commitments made under the AoC and RySG therefore supports the work of the WHOIS RT. The RysG recognizes the care and thought that has gone into the definitions. Due to existing workloads, RySG expects to provide further feedback shortly.</p> <p>RrSG: The expression <i>Consumer Trust</i> is a cause for concern and defining it will be challenging. The RT should adopt a temporary working definition that allows the group to move forward in its mission while continually working to create a more permanent definition eventually derived through a consensus process.</p> <p>IWGDPT: The IWGDPT draws the RT’s attention to a common position adopted on <i>Privacy and Data Protection Aspects of the Registration of Domain Names on the Internet</i>. See: www.datenschutz-berlin.de/attachments/222/dns_en.pdf. While some of the issues have been addressed through the creation of the .name gTLD and more privacy-friendly policies of some registrars, issues in the paper remain valid i.e.: 1) lack of purpose, definition and limitation for WHOIS data (including unlimited port 43 accessibility); 2) insufficient protection against secondary uses (including bulk downloads for offering value-added service and for sending spam); 3) Lack of transparency for registrants about how their data will be processed by registrars and registries.</p>
<p><u>Law Enforcement – Definition</u></p> <p><i>Law Enforcement shall be considered to be an entity authorized by a government and whose responsibilities include the maintenance, co-ordination, or enforcement of laws, multi-national treaty or government-imposed legal obligations</i></p>	<p>VOL: The term “law enforcement” is defined without making the scope clear: traffic wardens or NSA? The term “government” also needs to be defined.</p> <p>CAUCE: The definition does not distinguish between sworn law enforcement officials and other entities with the mentioned obligations. Law enforcement officers should be narrowly defined as individuals: 1) <i>who have been sworn or commissioned as a law enforcement officer by a government agency of competent authority;</i> 2) <i>who are charged with upholding the general criminal laws of an applicable jurisdiction, including having power to arrest;</i> 3) <i>typically have received specialized peace officer training (see submission for examples);</i> 4) <i>who normally receive tangible official signs of their role such as police uniform or official credentials.</i> Adjusting this definition does not mean to exclude non-sworn officials from the scope, they just need another label. It should also be considered whether law enforcement should include national intelligence services and national/multi-national military services.</p> <p>ECTA+M: The definition is very broadly drafted. Should private parties interested in enforcing civil law remedies fall within such a definition? If it is intended to refer to law enforcement in the sense of public agencies, then greater care needs to be taken in the drafting. Consideration needs to be given to the range of legitimate legal proceedings whether criminal, civil or administrative, for which access to WHOIS data or extended WHOIS data, should be available.</p> <p>RG: Such a definition will only be useful if it has been decided that the WHOIS service will have (or does have)</p>

	<p>some special and particular intended uses unique to <i>Law Enforcement</i>. No opinion can be given until a document has been presented into which the definition fits. Should this definition grant LEA access to certain types of WHOIS then it should be drafted broadly.</p> <p>IPC: The RT reads this phrase as limited to governmental enforcement agencies but there is no evidence that the AoC drafters intended this reading. The RT should focus on whether this implementation meets the legitimate needs for the enforcement of laws, which mainly depend on the efforts of private parties. Reliable access to WHOIS data plays a significant role in advancing the legitimate needs of enforcement.</p> <p>BC: The BC accepts the definition.</p>
<p><u>Applicable Laws – Definition</u></p> <p><i>Includes any and all local and national laws that regulate and/or control the collection, use, access, and disclosure of personally identifiable information. It may also include other relevant legal obligations, including U.N. Universal Declaration of Human Rights and the U.N. Guidelines for the Regulation of Computerized Personal Data Files.</i></p>	<p>VOL: Exclusion process should be defined: when local laws and a UN declaration conflict, which is applicable?</p> <p>ECTA+M: The definition is narrowly focused on questions of personal data. The RT must also consider other applicable laws for the broader protection of consumers and the public at large, including laws on child exploitation, regulation of drugs and medicine, infringement of IP rights, fraud prevention and spamming. Given that the scope includes promotion of consumer trust, the RT must look beyond registrants and consider global citizens as users of Internet and buyers of goods and services.</p> <p>LEX: Refine the definition as follows: <i>Includes any and all locally applicable laws and legislation in force that regulate and/or control use, access, and disclosure of personally identifiable information. It may also include other relevant legal requirements, including but not limited to U.N. Universal Declaration of Human Rights etc. National is too narrow: the regulatory system may imply transnational prescriptions (e.g. treaty of law provisions that locally apply). Legislation in force reflects more accurately the intended reach of regulation. Legal obligations relate to engagement, legal requirements or legal requirements and obligations might be appropriate formulations. Included but not limited to: avoid any possibility of an excessively restricted interpretation.</i></p> <p>CAUCE: The definition is relevant if focus is solely on registrant privacy. Since this aspect must be balanced against the need to protect citizens, the definition should be widened to recognize the applicability of all criminal and civil laws on WHOIS policy, including laws against child exploitation and child pornography, against obtaining financial information by deceit/“phishing”, against spreading malicious software, against online sale of controlled drugs, against IPR violations, against various fraudulent schemes and against spamming activities.</p> <p>IPC: This definition lacks the needed precision. The RT must focus on laws applicable to ICANN in carrying out this policy. It seems inconceivable that <i>any and all local [...] information are applicable</i>. Which law is</p>

	<p>applicable to a particular registry or registrar in carrying out contractual obligations to ICANN regarding WHOIS? It is not helpful to assert that every law related to personal data applies. The RT should give consideration to the ICANN procedure adopted to implement a supermajority vote of the GNSO and unanimous vote of the ICANN Board for dealing with any situation in which contractual obligations appear to conflict with a law applicable to the operations of the registry or registrar. See http://www.icann.org/en/processes/icann-procedure-17jan08.htm. The policy recognizes that there will frequently be ways for registrars/registries to conform practices with applicable law in order to comply with WHOIS obligations. AoC 9.3.1 should be read in the same way. <i>Other relevant legal obligations</i> is also imprecise. ENISA has concluded that the UN guidelines are <i>not legally binding, neither to natural persons, legal or countries</i>; see http://www.enisa.europa.eu/act/rm/cr/laws-regulation/dataprotection-privacy/un-guidelines and http://www.un.org/documents/ga/res/45/a45r095.htm. This falls short of establishing any legal obligation that could conflict with or override contractual obligations regarding WHOIS. The RT's mandate in this field is narrow; the broad and imprecise definition proposed for "applicable laws" will do little to assist the RT in carrying out its assignment. Unless it identifies a particular law that has impeded or threatened to impede ICANN's enforcement of existing WHOIS policy, it may not be necessary to reach agreement on a definition of "applicable law".</p> <p>BC: The BC accepts the definition.</p> <p>RrSG: This definition is adequate with the exception that UN declarations and resolutions are often non-binding and as such inappropriate for the RT's work. Non-binding resolutions do not meet the appropriate threshold for an applicable law and such references should be removed.</p>
<p><u>Producers & Maintainers – Definition</u></p> <p><i>Producers and Maintainers of WHOIS Data:</i></p> <ol style="list-style-type: none"> 1. <i>Producers: The individuals or organizations supplying contact data for inclusion into WHOIS data.</i> 2. <i>Maintainers: The WHOIS Review Team proposes to subdivide this category in to:</i> <ul style="list-style-type: none"> ○ <i>Data Controllers: Individuals or organizations that define the data to be collected, require its release, and govern its use. May or may not be directly involved in these functions.</i> ○ <i>Data Processors: Individuals or organizations engaged in the collection, storage, and release of data,</i> 	<p>CAUCE: The definition of "producers and maintainers" mixes parties and roles with different perspectives and interests. A "producer" may be 1) the registrant; 2) a proxy; 3) a registrar or hosting company; or 4) a registrations service provider acting as a contractor or agent for the registrar. These roles may also change over time. The definition leads to confusion and so does the definition of "data controllers", especially the final part of the definition.</p> <p>ECTA+M: The RT needs to remember that EU data protection rules only apply to individuals. Businesses and non-persons do not generally have any legal rights to "privacy" and this is reinforced by requirements in many countries for business to register their details in public registers. Whilst the <i>Producers</i> definition is broad, ECTA+M believe it is important for the RT to recognize the multiple players that may be involved in the registration of the domain and the scope for the provision of false or inaccurate data. <i>Maintainers:</i> ECTA+M recognize the use of language derived from EU data protection legislation, established in Europe for over 20 years with well-known meaning in the context of data protection. The RT should consider carefully how they intend to use this terminology to avoid unnecessary confusion.</p>

<p><i>according to the terms defined by the Data Controller. They do -not- determine the nature or use of the data that they collect or maintain.</i></p>	<p>IPC: This definition does not refer to AoC wording and there is no explanation on why a definition of these terms is needed. IPC recommends that the RT drop this definition.</p> <p>BC: The BC accepts the definition.</p> <p>RrSG: Support.</p>
<p><u>Consumer - Definition</u></p> <p>There is no single universally agreed definition of ‘consumer’, and legal definitions in different jurisdictions vary widely. Some are narrow and limited to ‘natural persons’, while others are broader and include various types of organisations.</p> <p>The WHOIS review team has been considering a broad interpretation of the term ‘consumer’, as this would allow a broad range of perspectives to be considered by the review team. This appears to be consistent with the intention of the drafters of the AoC.</p> <p>In the global sense, "consumer" may mean:</p> <ul style="list-style-type: none"> • <i>All Internet users including natural persons, commercial and non-commercial entities, government and academic entities.</i> <p>And specifically within the context of this review, a "consumer" w.r.t. WHOIS data and WHOIS Service may mean:</p> <ul style="list-style-type: none"> • <i>Any consumer that acts as a Producer of WHOIS data (see above), Maintainer of WHOIS data and provider of WHOIS Service (e.g. Registrars), or User of WHOIS data (e.g. – individuals, commercial or non-commercial entities who legitimately query the WHOIS data).</i> 	<p>ECTA+M: The definition of consumer with respect to the WHOIS review does not exclude any person. If this broad approach is intentional, it may be preferable to use a definition which can be understood by all <i>Consumers</i> (whether native English-speaker, familiar with WHOIS or not). Otherwise, discussions on possibly excluded persons may arise. On the other hand, in many jurisdictions the concept of “consumer” has well-established meanings that relate to natural persons acting other than in the course of business. In a common dictionary, a <i>Consumer</i> is a “person who purchases goods and services for personal uses”. The AoC refers to <i>consumer protection</i>. If the intention was to mean all Internet users, then the focus should be that on its natural and ordinary meaning.</p> <p>LEX: <i>Consumer w.r.t. WHOIS data and WHOIS Service may mean: any consumer that acts as a Producer of WHOIS data, Maintainer of WHOIS data and Provider of WHOIS Service, or User of WHOIS data (e.g. individuals, commercial or non-commercial entities who query or consult the WHOIS data).</i> Is it opportune to postulate the “legitimate” nature of the query/consultation? Anyone can consult WHOIS data, legitimately or not and we do not presume that there is an intention to exclude the non-legitimate seeker for data. Use implies query AND consultation.</p> <p>IPC: A broad interpretation is probably consistent with the intention of the AoC drafters. The first definition is sufficient but the second one is confusing and leads to the absurd conclusion that the goal of ICANN WHOIS policy should be to promote ICANN’s own trust in itself. Internet users rely upon accurate and accessible WHOIS data. The RT needs to apply common sense and conclude that public trust is diminished if this data is inaccurate, inaccessible and unreliable. The first bullet in the definition is consistent with this common sense definition and should suffice. The definition should not be limited to WHOIS users. The fact that domain owners are required to provide accurate ownership and contact data for Internet domain names has a deterrent effect against fraudulent, deceptive and illegal behavior and promotes consumer trust. No definition of Consumer Trust is needed. Consumer Trust - promoted by sound WHOIS Policy and implementation - is the expectation that actors on the Internet will be transparent and accountable for their actions. Users expect to be able to find out with whom they are dealing. If this is upheld, WHOIS can make a substantial contribution to consumer trust. If it undermines or erodes this expectation, it does not promote trust and thus fails the test set out in the AoC.</p>

	<p>BC: The BC supports a broad definition of the term consumer: the first definition.</p> <p>RrSG: The RrSG is concerned with the broad scope that <i>Consumer</i> may encompass. Creating an overly broad definition will complicate the further definition of <i>Consumer Trust</i>. The RrSG recommends that the RT construe the term narrowly in terms of WHOIS specifically.</p>
<p>Scope of Work and Roadmap https://community.icann.org/display/whoisreview/Scope+and+Roadmap+of+the+WHOIS+RT</p>	<p>ECTA+M: The non-exhaustive list of actions is sensible if conclusions are drawn about the effectiveness of WHOIS in relation to the AoC. In light of the new gTLD program’s potential for abuse, WHOIS needs to ensure that there is <i>timely, unrestricted and public access to accurate and complete WHOIS information</i>. ECTA+M recognize the need to balance privacy right of individuals with the public nature of WHOIS by: 1) Prohibiting anonymity for legal entities other than individuals; 2) Prohibiting anonymity for individuals where the domain name is business; 3) Allowing anonymity for domains registered in the name of an individual only where there is a means of contact. EU legislation stipulates that traders must identify themselves and their contact details on website. This should apply to domain registration in a business context. Reference is made to the criteria in EU’s E-Commerce Directive, see the contribution: http://forum.icann.org/lists/whois-rt/msg00008.html. Regarding IDNs, there is a need for the WHOIS records to be in standardized ASCII/English irrespective of whether the domain is ASCII/English or not.</p> <p>IPC: There should be a reference to the review of proxy and privacy registrations. They play an increasing role in the gTLD space and have grown from market need. The current ICANN policy regarding them undermines consumer trust and creates law enforcement concerns. A standardized process for the access to WHOIS data hidden with a proxy or privacy registration is long overdue. The RT needs to analyze the issues with registration data protected by a proxy or privacy service.</p> <p>ALAC: ALAC appreciates that the RT contextualized and centered its mandate on the AoC paragraph and the emphasis placed on <i>public interest</i>.</p> <p>BC: The BC supports the document and recommends that the RT identify specific examples of problems that have arisen due to restrictive, inaccurate or misused WHOIS. Examples should be highlighted and recommended mitigation measures included in the final report, as well as an assessment of whether ICANN is adequately using fact-based studies to inform WHOIS policy development. Over the years work has been done to define and advance these studies; see: http://forum.icann.org/lists/whois-rt/msg00016.html.</p> <p>RrSG: Support.</p>
<p>Outreach Plan https://community.icann.org/display/whoisreview/Outreach+plan</p>	<p>ECTA+M: ECTA+M fully support this plan for openness. Given the limited opportunities for geographical outreach, open access to calls, recordings and email is vital.</p> <p>BC: No issue with the outreach plan with the exception of the draft report release. Given that the application</p>

	<p>launch period for new gTLDs may coincide, it may be difficult for BC Members to devote the time needed for a thorough review of the work completed.</p> <p>RrSG: Support.</p>
<p>Action Plan https://community.icann.org/display/whoisreview/Action+plan</p>	<p>ECTA+M: ECTA+M trust the action plan will allow the RT time to process the public comments. The program of work should correlate to the scope to ensure that it meets the objectives of the review. Views should be sought from law enforcement agencies, consumer interest groups, brand owners and their representatives.</p> <p>BC: The BC recommends that the RT incorporate the collection of issues resulting from restrictive, inaccurate or misused WHOIS into the Action plan. The RT should review information already available from complete WHOIS studies (ask ICANN staff). The BC supports the inclusion of validated studies from external sources which provide such data.</p> <p>RrSG: Support.</p>