**Status Update Report from the Expert Working Group on gTLD Directory Services**
**Comments of the NCSG**

The Noncommercial Stakeholder Group thanks the EWG for its hard work and dedication of time, far beyond expected calendars and schedules. In the comments below, we applaud positive directions of the report, and would like to draw to your attention areas where there are issues which cause us concern.

Here are some aspects of the Report we regard as positive aspects from a noncommercial perspective:

> Gating -- creating gated or barred access to the personal and sensitive data of organizations, individuals, small businesses and large businesses from those who might misuse and abuse the data is a big step forward.
>
> Improving Registrant Privacy – with Binding Corporate Rules, support of Shield/Proxy/Privacy services, and Secured Protected Credentials creates important, critical even creative protections for the lives and well-being of Internet users. But we note it is an incomplete safety net, and we need far more protections for organizations with privacy protections under existing speech laws.
>
> Beyond ARDS – we support the movement of ARDS to exploration of RDS and the discussion from a single centralized repository to more diverse regional or thick registry repositories.

In a nutshell, here are our deep concerns for the Report:

Registrant Type – the introduction of a new field without rhyme or reason (mentioned only once in an appendix of the Initial Report) and yet one with enormous implications for organizations, individuals and companies operating in countries with Free Speech and Freedom of Expression laws (a large percentage of gTLD registrants).

Too Much Data – with so much centralization, and its incumbent security and speech risks, we would have expected the EWG to streamline the data to only that which is needed for the technical stability and security of the Internet (e.g., not physical address which can be obtained through due process after the technical crisis is handled). We hope we can see this streamlined data in the next version.

Unlimited Access to those with Credentials – we look at the proposals and to us, the appearance seems to be one of "unlimited all-you-eat-access" to the data once you have made it through the gate. That gate is not only for the investigative Law Enforcement representative, or the lawyer engaged in litigation, but to all within their organizations – including assistants, paralegals, and secretaries. We trust that is not the intent, as you are as aware as we are that insider abuse is a number one threat for most organizations with respect to confidential data. We comment further below re: the ongoing security

concerns of this data, even to those with credentials. The right to access once must not become unlimited right to access repeatedly, as each case and need is different.

**We follow the order of the EWG report for the remainder of this NCSG comment with some additional conclusions at the end.**

> Section III(b) Progress since the Initial Report; Interaction with subject matter experts and stakeholders"

We were among the commenters who encouraged the EWG to consult with more subject matter experts, including experts on Free Speech, Freedom of Expression and the rights that flow from these activities to organizations, individuals and companies. In our initial comments, we provided the names of leaders in this field, but have learned a bit to our dismay, they have not been interviewed.

Those who specialize in the abuse of the Whois data as well as the use of Whois data should be equally on the EWG target list of special interviews. We urge that these meetings take place ASAP for a full and fair report.

Interviewing experts who are data users has been done well; interviewing those Experts in the abuse of domain name data merits similar attention.

I. Community Input on the Initial Report, Section III(a)

We are concerned about Community Input. The EWG received only 35 substantive comments, of which 7 were ours (NCSG). In areas that have garnered dozens of passionate comments in the past, that seems a little low. There is traditionally a larger audience – including Data Protection Commissioners and privacy organizations – who have not spoken to ICANN – why?

We fear one reason is the name change from Whois to "Directory Services." It is not a shift that ICANN has communicated well to the outside world, and not one noted or tagged on the EWG website. It is even hard for us to find the proceedings. Certainly when you look through the history of the Whois debates and work in searches, the EWG materials do not arise.

The Whois Review Team spoke on this issue, and passed an Outreach recommendation that we urge the EWG to follow:

> **ICANN should ensure that WHOIS policy issues are accompanied by cross-community outreach, including outreach to the communities outside of ICANN with a specific interest in the issues, and an ongoing program for consumer awareness. (Recommendation 3, Outreach, Whois Review Team Final Report)**

ICANN Is the expert on this technology, so let's please use it to flag and tag and show the world, not deeply involved in our process that Directory Services is our next-generation Whois debate. Otherwise, the world will be upset when they learn.

II. Interaction with subject matter experts and stakeholders, Section III(b)

In our original comments, we requested outreach and discussion in private meetings by the EWG with subject matter experts specializing in the *protections* of user data and abuse of the Whois data. While we understand that the EWG has continued its many discussions with the law enforcement, security groups and other *users of the Whois data*, we have seen no meetings held with world specialists in the First Amendment and Freedom of Expression laws, or with those who face the abuses of Whois data every day on behalf of their client organizations, small businesses and entrepreneurs. Has the EWG met with data commissioners?

These experts include some within the ICANN community, including Wendy Seltzer, who founded the Chilling Effect Database while an attorney with the Electronic Frontier Foundation, as well as Kathy Kleiman, John Berryhill and Bret Fausett, as well as other UDRP defense attorneys, who should be called to share the stories of abuse of trademark in anti-competitive ways to drive out entrepreneurs, small businesses, and competition generally.

These meetings should certainly take place before the final report to give a balance to the EWG perspective – and legal expertise.

III. Proposed Categorization of Data Elements, Section IV(a), Step 1: Data Collection :

A. Too Much Data

Placing the names, addresses, emails and phone numbers of every gTLD Registrant in the world in a centralized database is both inappropriate and unnecessary. The goals of ICANN and the technical infrastructure under its management can be served well by a much more streamlined set of data.

The rest of the data retrieved from Registries and Registrars into a centralized or multiple regional databases should be that needed for technical solutions – for timely security and stability issues – not for every possible content question or investigation.

For the data has been pulled from the protections of its national law, and serves then only the purposes clearly within the scope of ICANN, namely security and stability. As discussed in all of our comments, we risk exposing Registrants worldwide to threats they do not even know they face, and allegations not even illegal in their own countries, but for which they will have no notice of the demand and collection of their personal and sensitive data (which includes physical address for all organizations, home-based businesses and individuals).

B. Registrant Type – the explosion of an unsupported field.

We support and appreciate the withdrawal of “Purpose” as a proposed field in the Initial Report of the EWG. But we raise very similar concerns about the addition of “Registrant Type” as a new field.

First we note that Registrant Type appears to have been mentioned only once in the EWG's Initial report, on page 45 of 48, in a latter appendix. There was no justification in the text, or clear description for the readers of the report. Now we see this field exploded in the Status Report and repeated as if it were an accepted and known fact. It is not.

The differentiation of individuals and legal entities serves no purpose within the ICANN system, and its automatic extension from some ccTLDs to the whole of the gTLD system raises risks the EWG has not even mentioned or balanced in either of its reports.

Basically, this differentiation of "individual" and "legal entity" divides the Registrant world into classes unsupported and overbroad under many national laws – including US law under which tens of millions of gTLD Registrants are protected.

Categorization of "individual" vs. "legal entity" implies a loss of rights when one becomes a legal entity that is simply unsupported by national law. Many businesses get special protection under national law, including small businesses, home-based businesses (including those run by seniors and "moms" both meriting additional protection), battered women shelters, Planned Parenthood medical offices, abortion clinics, schools educating girls in countries in which such an act is one of defiance and purpose, news organizations in and near countries where news is restricted, and all groups providing other forms of controversial, but protected information in the amazing marketplace of ideas that the Internet provides.

Such groups include further:

- Educational organizations, including for women and girls
- Pro-union organizations, many initially opposed by management
- LGBTQ groups,
- Charitable organizations of all flavors, "501(c)(3) organizations" in the US, and "legal entities" by law
- And every other organization or business created to share information, news, guidance and knowledge about religious, political, ethnic, moral and personal views that are different from their neighbors, co-workers, employers, apartment owners, universities and communities.

Many are incorporated as legal entities, and yet that in no way lessens their protections – or their need for protections. Free speech and Freedom of Expression laws protect them from the mandatory publication of their names and addresses for the speech in which they engage is far more important than the structure in which they appear. Further, confidentiality of the personal information of individuals is not the only "privacy' right that ICANN needs to accommodate; it has to accommodate confidentiality whose purpose is to protect other fundamental human rights, such as freedom of speech, freedom of association, anti-discrimination, and freedom of religion.

While we applaud the overall more nuanced approach the EWG has taken to the formidable job of mastering the complexities of directory services, unfortunately you appear to have fallen into a trap of looking at matters in a binary way, namely: person=possible privacy protection, organization=no privacy

protection. As indicated above, however, not only are there many other perfectly valid legal rights to confidentiality available in global law, but many privacy regimes acknowledge privacy rights for legal persons. This distinction is thus meaningless in this context, and must not be made.

**Thus, Registrant Type** in this Status Report is overbroad and underinclusive, and should not be included in the DNS. It flags for special treatment legal entities that, under many national laws, ***are protected from prejudice or special treatment.*** Specifically the US Supreme Court has written across five decades of the right of not only individuals, but organizations and companies not to publish their names and addresses as part of their speech. Specifically:

> "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. **Persecuted groups and sects** from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." *Talley v. State of California,* 362 U.S. 60 (1960) (emphasis added).
>
> "On occasion, quite apart from any threat of persecution, an advocate may believe her ideas will be more persuasive if her readers are unaware of her identity. Anonymity thereby provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent…. Thus, even in the field of political rhetoric, where "the identity of the speaker is an important component of many attempts to persuade," *City of Ladue* v. *Gilleo*, the most effective advocates have sometimes opted for anonymity." McIntyre vs. Ohio Elections Commission, 514 U.S. 334 (1995).
>
> **And most recently:** "Political speech is so ingrained in this country's culture that speakers find ways around campaign finance laws. Rapid changes in technology—and the creative dynamic inherent in the concept of free expression—counsel against upholding a law that restricts political speech in certain media or by certain speakers. … The Court returns to the principle established in Buckley and Bellotti that the Government may not suppress political speech based on the speaker's corporate identity. No sufficient governmental interest justifies limits on the political speech of nonprofit or for-profit corporations." Citizens United v. Federal Election Commission, [citation] (2009).

Domain names are clearly the "electronic pamphlet" of the 21st century, and it is a right of publication not only of individuals, but as pointed out in the Supreme Court language, of groups and sects (many of which are incorporated).

Thus, speech laws in the US and other countries with similar free speech/freedom of expression laws protect against the mandatory publication of name and addresses by organizations, association, agencies, affiliated entities, and companies large and small as well. For all of these organizations, companies and individuals engage in the free and full exchange of communication for research, education, policies, and ideas.

We understand this field may be intended to reveal the legal status of entities trading with end users – namely, buying and selling goods and services with customers. We note that national laws are taking

care of this issue as they are increasingly mandating the inclusion of name/address/complaint contact information on the homepage of a company selling/buying goods from consumers – just as a storefront in many physical marketplaces must post an "operating license." We believe this is the appropriate sphere of action of governments, to regulate e-commerce, this is not the role of ICANN. Arguments about the necessity to provide this information in domain name listings are, with respect, spurious.

However, the voluntary disclosures of companies in the Whois Directory Service databases are hereby supported – and the eBays, PayPals, Macy's, Harrod's and The Mashbir, by way of example. If these companies want to disclose additional information, and teach consumers to look for that additional information prior to purchasing online, as set out in parts of the EWG report, that's a direction and option we support. It must not be mandatory, nor should there be any implication that failure to put data in the Whois means the organization is acting outside the law.

c. Principles for Data Collection – Table on pages 12 and 13

We highlight Principles that deeply concern us and note questions about the meaning and purpose of others.

1. Registrant Type- for all the reasons set out above, we deeply oppose this one.

2. Registrant Postal Address

We see few benefits, but many dangers for this inclusion in the ARDS or RDS. For purposes of security and stability, finding a Registrant contact as quickly as possible makes sense – and an email and/or telephone number, as well as IP address, will provide much information. But address, including for the billions of new Registrants coming online in the gTLD program, New gTLD program, and especially the IDN Program (Internationalized Domain Name), the address provides no viable or rapid contact.

But it does provide exposure as a new business creates a good or service that challenges a larger player in a region, or as a school offers education to girls in certain regions, or as access to health care and birth control challenges certain mores in certain cultures.

So Registrant Postal Address is best left to the Registries and Registrars who already have procedures for verifying and validating that their disclosure of sensitive data, including credit card numbers and credit card addresses, are released pursuant to the laws of their country and often in conjunction and cooperation with their local law enforcement officials.

In a centralized repository or repositories, the movement of this data from its national protections, and the release of it across gTLDs (rather than the one gTLD of a current or future Thick Registry) severs it from national protections and leads naturally to the disclosure of all pro-democracy groups to rogue state law enforcement, all Jewish department stores to Iranian police, or even the address of all girls' schools in Pakistan to whoever manages to get credentials from the Taliban.

These are not extraordinary requests or intended to be explosive, but the natural and logical outgrowth of the inclusion of the physical address field and its separation from the protection of national law.

3. Principle 2 is unclear

As the Interim Report has not returned to Permissible Purposes, it is hard to evaluate the scope, breadth and meaning of Principle 2. This is a key issue, as permissible purposes illuminate much of the rest of the report, so we anticipate having another opportunity to elaborate our comments once the final report has been prepared.

We raised strong objections to an overly-broad set of Permissible Purposes in our first comments, http://mm.icann.org/pipermail/input-to-ewg/attachments/20130822/186e4f03/UseCasesFundamentallyFlawed-0001.pdf, and renew and heighten those comments today. Any system that allows any individual to access the physical address of any domain name registrant is overbroad. Uses by third parties cannot drive the purposes for which that personal and sensitive data was given in the first place (including name, physical address and telephone number). ***We have to return to the initial purpose for which the Whois data was given – a technical purpose consistent with rapidly solving security and security stability problems involving domain names.***

d. Data Disclosure Principles – Table on pages 13 and 14

It is unclear what is Registrant-supplied data and Registry/Registrar-supplied data. Particularly when Registrant Type (deeply opposed for the reasons above) and Registrant Contact ID appear to be both Registrant-supplied and mandatory for publication, we don't under stand how the principle of "Registrant-supplied data should be gated by default," applies.

We further note that the EWG notice, ***Tel# is mandatory to collect but not to disclose*** is a good one, but not a principle that seems to have been applied across the EWG reports and tables. We support this Data Disclosure principle, and its consistent application across all EWG work and proposals.

e. Domain Name Purpose

We strongly support the removal of the proposed field of Domain Name Purpose and thank the EWG for listening closely to public comment and concern on this issue. We agree that voluntarily "opt-in" procedures could be made available. We agree that such a field would be nearly impossible "to globally enforce."

f. Resulting Data Classifications

This is a difficult table to read. According to our understanding, we submit:

- Registrant Type should be discarded,
- All Role-Based Contacts with optional information should be an **Opt-In rather than an Opt-Out**, to ensure that organizations, individuals and small-businesses know their rights, and choose to publish their address, phone number, fax, email and other contacts openly, willingly and

knowingly. Opt-in is a good and safe option, especially in dealing with those organizations, individuals and small businesses that operate without legal counsel and without deep knowledge of this data and where/how it will be used.

- As discussed thoroughly above, EWG should not include a Registrant Type. Accordingly, and per its comment of page 18, it should not consider additional fields to be collected or disclosed. The risks and the bypassing of national law speech and expression protections would only be aggravated and expanded.

g. Proposed User Accreditation for Access to Gated Data

The EWG Report shares you have "consulted with Europol, Interpol, and other members of the global Law Enforcement Community." But have you consulted with Rebecca MacKinnon and others in Global Voices Online who specialize in the political voices, and the many governments who seek to limit them? Once this data is centralized into an ARDS or multiple RDS, as discussed above, the protections that Registrars and Registries provide under national law are eliminated. We strongly suggest that you also consult with other stakeholders who are expert in the kind of pressure that some parties will bring to bear on this newly accurate registry, stakeholders such as Transparency International (http://www.transparency.org/country), the OECD Anti-corruption Directorate (http://www.oecd.org/corruption/keyoecdanti-corruptiondocuments.htm), and the Article 19 group (http://www.article19.org/). ICANN is, after all, a multi-stakeholder organization.

Additional Gated Access Principle #1: Accordingly, the "accreditation scheme" should certainly be more than "minimum." It must be sufficient to show who is requesting the credential, and who will be responsible for the use and any abuse and misuse of the Whois data. We do not see these checks or even principles in the Status Report. Certainly access to a database of the nature of the ARDS/RDSs requires the "strongest" of credentialing systems – not a mere minimum. This minimum credentialing seems to defy the very concept of checks and balances, benefits and risks, that the EWG is putting forward as it submits the ARDS/RDSs as a better option.

Additional Gated Access Principle #2: What is "self-accreditation" and why should we allow it? As discussed throughout this report, and by those who specialize in the Abuse of the Whois Data if the EWG would only invite and meet with its Experts, there are heavy incentives to abuse and misuse Whois data and a "self-accreditation" process by the Data Requestor seems set to allow an unlimited back door without checks, balances or protections. Clearly the Data Requestor needs the highest form of check and review.

Additional Gated Access Principle #7: We support the agreement of any and all credentialing organizations to laws and frameworks requiring due process, accountability, security, fair access and adherence to applicable law – and note that the ARDS and/or multiple RDS may or may not exist in countries with strong laws and due process procedures. As a principle, the EWG must mandate that an ARDS and/or multiple RDSs must exist in a nationality with strong data protection and due process laws

that apply to all parties, not just their own citizens. Otherwise, many of the proposed protections assumed within this report fall apart.

Additional Gated Access Principle # 8 simply cannot be right. If one attorney has access for a law firm, all of her paralegals, secretaries and clerks will have the same access? If one member of a Law Enforcement organization (of 10 or 10,000 employees) has access to the ARDS/RDSs, then all other agents, deputies, assistants and others will have access as well – be it the FBI or Rogue state Law Enforcement?

That cannot be right. For accountability and transparency, credentials must be given to individuals who would be responsible for each and every access. Certainly, their organizations, once checked, will matter to that credentialing process, but the responsibility, accountability and authority of one person must be tied not only to the registration of that credential – but each and every use. For purposes of the integrity and security of this system, there cannot be a blanket authorization for everyone in an organization.

Footnote 9 is ambiguous: As the representative of hundreds of Registrant organizations, we ask what the EWG means by "Registrant Approval," and how Registrants would even know or be involved in the verification process? Is the EWG recommending a Registrant Approval of requested credentials? How would that process work; what specific proposals are being made? This seems a baffling proposal.

Additional Gated Access Principle 14 Needed: Jurisdiction

Each request of a Person/Entity Requesting the Data must prove that the reason for the data requests is a violation of the law in the Jurisdiction in which the Registrant operates or lives. The EWG proposes that this jurisdictional information be available for Registries, Registrars and Registrants. We propose this as Additional Gated Access Principle #14.

For what is a civil violation in country A is not in country B, e.g., comparative advertising is illegal in Germany, but not in the US. Further, what is a criminal violation in Saudi Arabia or China, is protected by Free Speech and Freedom of Assembly in the US. So there is a possibility of violating a Registrant's rights and protections for reasons not consistent with the national laws under which they are operating.

Additional Gated Access Principle 15 Needed: Access not unlimited

We have read the principles many times, and see no bar to "all you can eat" access – the ongoing and repeated use of the ARDS/RDS data for both valid and invalid purposes. The Requestor, for each, request must meet the high threshold of disclosure for each and every Registrant is entitled to its/her/his own level of protection.

We would like to see a full ***multi-stakeholder*** risk assessment for the next iteration of the proposed ARDS/RDS, with potential mitigations. We would like to see proposals for routine audit, and how the EWG proposes to deal with the inevitable requests from investigators of all types, to obscure or delete their own audit and traffic pattern trails. The devil lies in the details.

h. Summary of Key Benefits

In addition to the Summary of Key Benefits of page 22, the final EWG Report should include a fair and balanced **Summary of Key Risks**. The full cost/benefit/risk equation should be clearly set before the ICANN Community, and the EWG is in the best position, by far, to conduct and share this analysis.

i. Improving Data Quality

WE do not support the ARDS/multiple RDSs engaging in a standard validation of data. The Registrars have already committed to a detailed process of validation and verification in the 2013 RAA, which we believe may be overly broad. We expect the incentive of offering New gTLDs will be an enticing one and many will continue to sign this updated agreement.

But as the EWG knows, validation of physical address is not a requirement of the 2013 RAA and for good reason: it is hard, difficult and sometimes impossible to check this information, and Registrars have access to much more useful location information through the credit card numbers they collect and the additional data supplied to and through credit card companies.

ARDS/multiple RDSs should not require the physical addresses of Registrants, for all the reasons discussed above. Should it choose otherwise, physical address is certainly not a field to be mandatory in its validation due to expense, impractical and unintended, but dangerous results.

Addresses are hard to create and standardize. By way of example, in the US, many rural and suburban street addresses did not come into being until the last few decades—their creation propelled by a specific "911" project where US as a national priority wanted a telephone system that could automatically route the address of the caller to emergency services (police, ambulance, fire trucks). To that end, rural areas received street names, numbering systems were implemented and a national push was made. The effort was difficult and costly, but driven by a national goal.

Many countries have no such national imperative and many have no good physical addressing system across the whole of their population. So to "verify" an address in many regions of the world will be tremendously costly and even impossible in many countries and regions of the world. We foresee Registrants losing domain names in countries without clear and precise street-labeling and addressing systems. It is a problem the Registrars raised repeatedly in the RAA negotiations.

Yet, these are the very regions where the Internet offers the most potential for growth, and the most opportunity for positive change. These are the regions where a domain name promises a huge difference in status – for those seeking to move from "users" of the Internet to "content makers and providers" of the Internet, actively posting and sharing ideas, thoughts, advocacy, and more. Domain names are key for the expanding entrepreneurs, organizations and enterprising organizations and individuals seeking out a new role – a key for millions coming online who may or may not be able to prove their address to Western standards. Will domain names for these individuals, organizations and small businesses be lost? That seems a strange result for such a critical medium.

However, voluntary validation is an option – and opt-in data that a Registrant my choose to provide and choose to pay for additional validation – may be a good option and middle ground on this issue.

e. Principles Related to Contact IDs

We seek to better understand Contact IDs – and to what extent organizations, small businesses and individuals will have access to this Contact ID, or whether it will be a service provided to and paid for by larger companies. We look to the EWG for clarification and discussion before final decision.

*We would like to see the summary of Key Benefits balanced by a "Summary of Key Risks." If it is at this point impossible to come up with that summary of key risks, we urge the EWG to conduct a full,* ***multistakeholder*** risk assessment.

f. Improving Registrant Privacy

We support the EWG statement that registrants of all type deserve privacy. We note that individuals and "some businesses" are mentioned, and urge the EWG to include the full scope: individuals, companies and organizations (the 3 type of Registrant groups represented within ICANN) in its Final Report, in its discussion and on page 31.

We strongly support the following strong steps by the EWG in the data protection area:

1. Binding Corporate Rules.

We completely agree that: "As a major player in the ecosystem of the Internet, and as the multi-stakeholder group which sets policy for the collection, use and disclosure of personal information related to domain names, it is important for ICANN to show corporate responsibility in promoting global compliance with best practices in data protection."

As noted in the EWG report, "the European Union has now agreed on what needs to be found in binding corporate rules for international corporations and entities which hold and transfer personal data" (page 32). This will be a critical step forward when ICANN adopts it as the request of the EWG. It will create better compliance with the data protection laws in the many countries that have these national laws, including Japan, S. Korea, Canada and the European Union nations. Given the current crisis in Internet governance, it is high time that ICANN indicated its global understanding of relevant data protection law around the world, and adopted binding corporate rules that harmonize its data protection practices in a manner that meets the standards expected by the many jurisdictions with data protection law. While we note that the issue of binding corporate rules is under discussion at the EU in the context of impending data protection regulation, this is no reason for ICANN not to move forward, as an international organization operating in jurisdictions with data protection law that applies not just to customers, but to staff and volunteers as well. This action is long overdue and we applaud the EWG for raising it.

2. Shield (Privacy) and Proxy Services

The ongoing use and availability of Shield (Privacy) and Proxy Services is now an established fact of the DNS landscape. It is an also an area of active and involved MultiStakeholder work within the GNSO at this time. Every Stakeholder Group, as well as representatives of ALAC and GAC, are actively involved in discussing Accreditation, Relay, Reveal, Takedown and Publication of the Whois data, in a very detailed manner.

Accordingly, we urge the EWG not to adopt principles in these areas as those principles may conflict with work now in progress, but rather support the 2013 RAA as a framework and starting point (as the Suggested Principles for Enhanced Protected Registration Data" tend to do.

But the "Suggested Model and Principles for Reveal and Relay are too detailed and proposed without the balance of any Free Speech and Freedom of Expression attorneys or representatives on the EWG. This is an area in which the balance of the GNSO Multistakeholder Process should take the lead.

Even the "Relay" request fails to acknowledge the types of abuse now being raised in the GNSO Proxy/Privacy Accreditation Working Group: including the need of a Proxy/Privacy Provider to be able to act on those misusing or abusing the Relay process – including those engaged in spam, sending invalid requests via bots and automation, sending frivolous requests or engaged in a pattern of abuse against Registrants (as some Registrars and Proxy/Privacy Providers are finding some divorce attorneys, for example, prone to do).

Especially the "Escalation" procedures are too detailed, reflecting a particular process some may want, not reflecting a tendency of abuse that some experience, and calling for action that may or may not correspond to what the GNSO WG (PPSAI) ultimately recommends.

We ask the EWG to step back on this issue, and allow all details of this accreditation process to work through the active, robust, diverse GNSO process now in full swing. We also call on the EWG to take a look at The Chilling Effects Database, at http://www.chillingeffects.org/, and run by the Electronic Frontier Foundation (EFF), Harvard Law School's Berkman Center, Stanford Law School's Center for Internet & Society, Boalt Hall's Samuelson Law, Technology and Public Policy Clinic, and other law schools

> "to see how vague "proof of wrongdoing" can be, how broad allegations of illegality can run, and how baseless, threatening and intimidating some letters can be. They create a "chilling effect" which must be a priority of the ICANN Community and EWG to prevent."

Clearly both sides need to balanced, we again urge the EWG to engage with experts who specialize in the Abuse of the Proxy/Privacy System and Whois data generally.

f. Secured Protected Credentials.

Here is something we applaud. Secure Protected Credentials are one of the great introductions of the EWG. They are a critical concept to going forward with Whois database and its future renditions. It is a classification that will support dissenting opinion, and especially most at risk – those called upon to object to their own governments, to seek the deepest political changes, and with their families and person most at risk of arrest, physical harm, or worse.

We urge the EWG to adopt specific recommendations calling on ICANN to devote staff and funding for this critical project and ensure that it takes the next steps forward – in conjunction with the UN or other organizations.

1. However, the suggested reach of the Secured Protected Credentials includes many Registrations best protected under Enhanced Protected Registration Services; as so many Commenters agreed, SPCs are for the worst of the worst.

Commenters appear to support Secure Protected credentials as a very limited proposal. Critical, but limited, we submit that only a limited number of organizations, companies and individuals will qualify, and these are likely to include undercover law enforcement, battered women shelters, and well-known dissident groups.

But we do not foresee every Religious Minority group, every Political Speaker, every Ethnic and Social Groups, every LGBTQ group, or everyone with a minority, unusual or radical idea obtaining a Secured Credential. Yet, as discussed above, these organizations, individual and corporate speakers are given protection and barred from having to give their name and address as a condition of speaking by Free Speech and Freedom of Expression laws. This includes domain name registrants involved in speech, advocacy, information, education, research and more.

Most of the ***groups the EWG mentions under Secure Protected Credentials are best protected, and merit protection, under the Enhanced Protected Registration Service,*** **with the most exposed and life-threatening situations protected by** Secured Credentials.

Accordingly, NCSG strongly requests that the EWG endorse two sets of laws for the proposed **Enhanced Protection Registration Service**, made available to and recommended by the EWG for:

- those protected by their national data protection laws; and
- and those protected by their national free speech and freedom of expression laws.

This will ensure that the robust exchange of ideas, majority and minority views, religious diversity and protection, political ideas and differences, education, research, ethnic and moral ideas and exchanges continue in a robust and active manner.

Thus, the “Analysis of Jurisdictional Issues and Applicable Law” should be expanded to include the US First Amendment, UN Declaration of Human Rights, and other documents of national and international standing on similar views – to ensure the full range of “sensitive data” protections accorded not only to individuals, but organizations and companies under treaty.

In Conclusion

We thank the EWG for its time and efforts, and look forward to meeting with you in Singapore.

Respectfully submitted,

The Noncommercial Stakeholder Group