ICANN CCWG-Transparency Work Stream 2

Executive Summary

This Report is the result of a multi-stakeholder consultation that was carried out by the Cross Community Working Group (CCWG) of the Internet Corporation for Assigned Names and Numbers (ICANN). It contains a set of targeted recommendations aimed at improving transparency at ICANN based around three main issues: reforming the ICANN's Documentary Information Disclosure Policy (DIDP), expanding proactive disclosure of information and boosting whistleblower protection.

The Report begins with a discussion of the right to information as a human right, to make the conceptual case for why this should apply to ICANN. Although it is broadly understood that the right to information applies equally to non-governmental organizations that serve a fundamentally public purpose, it is also worth noting that there are many benefits to a robust transparency system, including facilitating public oversight over decision-making, generating a strong system of accountability, and facilitating public engagement. Given ICANN's long struggle to battle public misconceptions about its role, functions and governance, transparency will be a key ingredient in countering misinformation and rumor.

The first section analyses the DIDP. Our consultation revealed strong support for major improvements to this policy. Among the most important proposed changes are bolstering the requesting procedures, including requirements that requesters should only have to provide the details necessary to identify and deliver the information, and a responsibility for ICANN staff to assist requesters as necessary, particularly where they are disabled or unable to identify adequately the information they are seeking. We also recommend that timeline extensions should be capped at an additional 30 days. We recommend that several of the exceptions be narrowed, so that they only apply to material whose disclosure would cause actual harm, and that the exception for vexatious requests should require consent from the Ombudsman before it is invoked. Importantly, we also recommend enhancing the independence of the appeals model by establishing a three member external review panel that will operate on an on-call basis. We also recommend that the Ombudsman's promotional mandate with regard to the DIDP be expanded, and that they should assume a monitoring and evaluation role, including tracking and reporting basic statistics on the DIDP's use.

The second section discusses matters that ICANN should proactively disclose. As a prominent entity in the broader internet governance ecosystem, ICANN has and will continue to engage with government stakeholders to inform, educate, and, from time to time, advocate for particular policies. Because ICANN represents the entire multistakeholder community, it is important for the entire ICANN community to know how and to what extent ICANN interacts with governments outside the traditional and formalized engagement via the Governmental Advisory Committee (GAC). Such transparency will allow such insight and possibly ameliorate concerns within the community that ICANN engages with governments above and beyond its engagement with other stakeholders and/or outside its remit. While

ICANN currently is obligated under U.S. federal law to report any and all federal "lobbying" activity, such reports are limited in their utility. First, reports filed under the federal Lobbying Disclosure Act (LDA) apply only to federal "lobbying" activities, thus not capturing any U.S. state or international interactions. Second, the reports do not encompass engagement with government officials that falls outside the statutory definition of "lobbying" [1] or fails to meet certain statutory thresholds. In light of these deficiencies, the Transparency Subgroup recommends certain additional disclosures that will complement ICANN's U.S. federal lobbying disclosure and provide a clearer picture of how, when, and to what extent ICANN engages with governments. This information may also better inform the Empowered Community if/when it challenges any ICANN Board action. Indeed, the CCWG-Accountability in its final report asked for such transparency. [2] ***[Note to readers – we're planning on expanding this section out a bit, to a broader discussion of proactive disclosure].***

The third section discusses ICANN's whistleblower protection framework. WS2 Transparency appreciates that ICANN responded to a recommendation from the second Accountability and Transparency Review and retained NAVEX Global to conduct a review of ICANN's Anonymous Hotline Policy and Procedures. Overall, we feel that NAVEX produced a very solid analysis of Hotline policies and procedures and proposed appropriate recommendations for improvements. We urge that the NAVEX recommendations be implemented by June 2017 as they address several concerns we share about the need for improvements in policies and procedures. These concerns pertain to: (1) the clarity and availability of the existing policy and employee education around it; (2) the definition of incidents report, which we feel is too narrow; (3) the Hotline policy scope; (4) the operation of the hotline process; (5) addressing fear of retaliation more effectively; (6) and the need for regular third-party audits. We offer specific recommendations in the concluding summary.

The Background section was drafted by Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy, and a Co-Rapporteur of the Working Group on Transparency. The section on the DIDP was drafted by Michael Karanicolas based on consultations and input with the community. The section on Proactive Disclosure was drafted by Chris Wilson, based on consultations and input from the community. The section on Whistleblower Protection was drafted by Barbara Wanner, based on consultations and input from the community.

[1] The LDA defines "lobbying" as lobbying contacts and any efforts in support of such contacts, including preparation or planning activities, research, and other background work that is intended, at the time of its preparation, for use in contacts, and coordination with the lobbying activities of others. For additional guidance re the LDA, please see http://lobbyingdisclosure.house.gov/amended_lda_guide.html

[2] Such calls for more transparency also derived from community angst associated with ICANN's former CEO's engagement with Chinese authorities in late 2015 and early 2016 with regard to China's World Internet Conference, as well as the former CEO's engagement on behalf of ICANN with Brazil concerning the creation of the April 2014 NetMundial conference.

Background on Transparency and the Right to Information

Institutional transparency is, in many ways, an emergent and evolving concept. Over the past two decades, the right to information has gone from being viewed primarily as a governance reform to being broadly recognized as a fundamental human right, protected under Article 19 of the United Nations' *Universal Declaration of Human Rights*,[3] as well as the freedom of expression guarantees found in other international human rights treaties. These include, for example, the *Charter of Fundamental Rights of the European Union*, where the right to information is enshrined under Article 42.[4] The right to information is also protected under the *American Convention on Human Rights*[5] as a result of the case of *Claude Reyes and Others v. Chile*.[6]

The recognition of the right to information as a human right has also been accompanied by the development, through jurisprudence and international standard setting, of established better practices in the implementation of this right. At the core of this emergent understanding of the right to information is the basic idea that the people, from whom all legitimate public institutions ultimately derive their authority, have a right to access any information held by or under the control of these institutions. Although, for the most part, this idea is focused on governments and related public bodies, it is broadly understood that the right should apply equally to non-governmental organizations that serve a fundamentally public purpose, such as where a government privatizes the water or power utilities.[7] Many right to information laws take this a step further, and attach transparency obligations to any private organization involved in delivering rights. For example, Kenya's Access to Information Act, the world's most recent, applies obligations to any private entity or non-state actor that is in possession of information where the release of the information may assist in exercising or protecting any right.

However, beyond cases where they are legally mandated to do so, many international organizations have embraced the right to information as a core responsibility. Right to information policies have been put into force in many international financial institutions, including the European Investment Bank,[8] the Asian Development Bank,[9] the Inter-American Development Bank[10] and the African Development Bank,[11] as well as UN institutions such as

---

[3] UN General Assembly Resolution 217A(III), 10 December 1948. The entrenchment of the right to information as part of freedom of expression was cemented by the UN Human Rights Committee (HRC), General comment no. 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34, available at: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[4] Adopted 7 December 2000, Official Journal of the European Communities, 18 December 2000, C 364/01. Available at: www.consilium.europa.eu/uedocs/cms_data/docs/2004/4/29/Charter%20of%20fundemental%20rights%20of%20the%20European%20Union.pdf.

[5] Adopted at San José, Costa Rica, 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.

[6] 19 September 2006, Series C No. 151, para. 77 (Inter-American Court of Human Rights). Available at: www.corteidh.or.cr/docs/casos/articulos/seriec_151_ing.doc.

[7] See, for example, right to information laws in force in Mexico, Nicaragua, Moldova, South Africa, Ukraine, Bangladesh, Kosovo, Colombia, Bosnia and Herzegovina, Georgia, Armenia, Estonia, Ireland, Guatemala, Argentina, Nigeria, Rwanda, Serbia, Ecuador, etc.

[8] *European Investment Bank Group Transparency Policy*, March 2015. Available at: www.eib.org/attachments/strategies/eib_group_transparency_policy_en.pdf.

[9] *Public Communications Policy*, 2005. Available at: www.adb.org/site/disclosure/public-communications-policy.

[10] *Access to Information Policy*, April 2010. Available at: www.iadb.org/document.cfm?id=35167427.

UN Environment Programme,[12] the UN Children's Fund,[13] the World Food Programme,[14] UN Population Fund[15] and the UN Development Programme.[16]

There are pragmatic reasons why so many international non-governmental institutions have embraced the right to information. A key benefit of a robust right to information system is its role in combatting corruption and mismanagement, by allowing broad oversight over decision-making and generating a sense of public accountability among staff. Similarly, the right to information is an important ingredient in generating trust in institutions, and facilitating dialogue with the public. For international organizations, which often need to engage with an even wider and more diverse network of stakeholders than governments do, the right to information is a key mechanism for fostering open discussion about their strategies and goals. This last point is of particular relevance to ICANN, which for years has battled public misconceptions about its role, functions and governance. The best answer to misinformation and rumor is openness and transparency. Sunlight is not only, as Louis Brandeis once famously said, the best disinfectant, it is also a fundamental ingredient to building trust in ICANN as stewards of a global public resource.

[11] *Group Policy on Disclosure of Information*, October 2005. Available at: www.afdb.org/fileadmin/uploads/afdb/Documents/Policy-Documents/10000004-EN-THE-AFRICAN-DEVELOPMENT-BANK-GROUP-POLICY-ON-DISCLOSURE-OF-INFORMATION.PDF.
[12] UNEP Access-to-Information Policy (Revised), 6 June 2014. Available at: www.unep.org/environmentalgovernance/UNEPsWork/AccesstoInformationPolicy/Revised2015/tabid/1060867/Default.aspx.
[13] UNICEF, Information disclosure policy, 16 May 20111. Available at: www.unicef.org/about/legal_58506.html.
[14] WFP Directive on Information Disclosure, 7 June 2010. Available at: documents.wfp.org/stellent/groups/public/documents/newsroom/wfp220973.pdf.
[15] Information Disclosure Policy, 2009. Available at: www.unfpa.org/information-disclosure-policy.
[16] Information Disclosure Policy, 1 October 2015. Available at: www.undp.org/content/undp/en/home/operations/transparency/information_disclosurepolicy.html.

Subtheme 1: Reforming the DIDP

Early on in our consultations, it became apparent that there was strong support for major improvements to ICANN's Documentary Information Disclosure Policy (DIDP). Many of our constituents, having had extensive experience with strong and effective right to information systems at the State level, were keen to explore how the DIDP can be brought into line with these good practice models. Fortunately, in designing a strong right to information policy there is a rich body of international standards to draw from. Although most of these ideas were developed in the context of governmental right to information systems, many of them are easily adapted to suit ICANN's unique operational context. Moreover, an increasing number of international organizations, such as UN agencies, international financial institutions (IFIs), and even NGOs, have adopted right to information policies of their own, providing a wealth of source material to draw on.

A strong right to information policy should begin by recognizing a right of access, which applies to all information held by, generated by or for, or under the control of the organization. It should also note, as an interpretive guide, that the organization's operations should be carried out under a presumption of openness.

The DIDP begins by noting that it guarantees access to "documents concerning ICANN's operational activities, and within ICANN's possession, custody, or control". This is a relatively wide definition, though in order to ensure broad applicability, the caveat that the policy applies only to "operational activities" should be deleted.

Strong right to information policies include clear and simple procedures for making and responding to requests for information. The world's best right to information policies spell these out in detail, and in many cases a substantial proportion of the law or policy is devoted to this explanation. However, ICANN's description of the procedures for access is conspicuously skeletal, stating only that:

> **Responding to Information Requests**
> If a member of the public requests information not already publicly available, ICANN will respond, to the extent feasible, to reasonable requests within 30 calendar days of receipt of the request. If that time frame will not be met, ICANN will inform the requester in writing as to when a response will be provided, setting forth the reasons necessary for the extension of time to respond. If ICANN denies the information request, it will provide a written statement to the requestor identifying the reasons for the denial.

This provision should be expanded to include clearly defined procedures for lodging requests for information, including requirements that requesters should only have to provide the details necessary to identify and deliver the information. The DIDP should also impose clearer guidelines on ICANN for how to process requests, including a commitment to provide reasonable assistance to requesters who need it, particularly where they are disabled or unable to identify adequately the information they are seeking. The DIDP should also commit to complying with requesters' reasonable preferences regarding the form in which they wish to access the information (for example, if it is available as either a pdf or as a doc). While these guidelines may already be spelled out in ICANN's internal procedural guides, it is also important to include this information as part of the DIDP, to ensure that requesters have a clear idea of what to expect.

Another problem with the DIDP is the timetable for response. 30 calendar days is generally reasonable, though it is worth noting that many countries, including Serbia, Denmark, Lithuania, Bulgaria and Indonesia, commit to responding to right to information requests within two weeks. However, while it is not uncommon for policies to grant institutions a degree of leeway regarding timeline extensions, the fact that there is no outside time limit for these extensions is a glaring problem. Many countries, such as India, do not allow for extensions at all past the original thirty day limit. However, among those that do, the vast majority cap extensions at an additional thirty days or less. If ICANN requires more than sixty days to process an information request, this is likely an indication that staff are not properly prioritizing DIDP requests, in line with the institutional importance of transparency, or that ICANN's record management processes need to be improved. Strong right to information policies generally also state that information should be provided "as soon as possible", in order to provide a clear indication that employees should aim for speedy disclosures.

Another major problem with the DIDP provision quoted above is that it only commits to responding "to the extent feasible, to reasonable requests", which implies that staff have discretion to abandon DIDP requests if competing work pressures are too intense, or if they feel that the request is unreasonable. The former is obviously incompatible with a robust transparency policy, while the latter is unnecessary in light on an existing exception allowing for dismissal of vexatious or unduly burdensome requests. The phrase "to the extent feasible" should be deleted, as should the word "reasonable".

Probably the most controversial aspect of the DIDP, according to our consultations, is the list of exceptions. Every right to information regime has exceptions to disclosure to protect information whose release would be likely to cause harm to a legitimate public or private interest. This is perfectly reasonable, and indeed essential to a robust and workable system. However, in line with the broader presumption of openness, these exceptions must be crafted carefully, and should only exclude information whose disclosure would cause real harm. Under international law, exceptions to the right to information should be based on the three-part test for restrictions on freedom of expression set out in Article 19(3) of the *International Covenant on Civil and Political Rights* (ICCPR).[17] This recognises restrictions as being legitimate only where they are: i) prescribed by law; ii) for the protection of an interest that is specifically recognised under international law, which is limited to the rights and reputations of others, national security, public order, and public health and morals; and iii) necessary to protect that interest.

In the specific context of the right to information, this translates into a similar three-part test, as follows:

- The information must relate to an interest which is clearly defined in law and which falls within the scope of the interests recognised under international law.
- Disclosure of the information may be refused only where this would pose a risk of substantial harm to the protected interest (the harm test).
- The harm to the interest must be greater than the public interest in accessing the information (the public interest override).

The three parts of the test are cumulative, in the sense that an exception must pass all three parts to be legitimate, and together these constraints reflect the idea that restrictions on rights

[17] Adopted by UN General Assembly Resolution 2200A (XXI), 16 December 1966, entered into force 23 March 1976.

bear a heavy burden of justification. It is clear that only exceptions which serve to protect the interests recognised under international law may be legitimate. This narrow list ensures that only interests of significant weight may trump the right to information.

The harm test flows directly from the requirement of necessity in the general test for restrictions on freedom of expression. If disclosure of the information poses no risk of harm, it clearly cannot be necessary to withhold the information to protect the interest.

Finally, the idea of weighing the public interest in openness against the potential harm from disclosure also flows from the necessity test. It is widely recognised that this part of the test involves a proportionality element. Thus, the European Court of Human Rights has, in the context of freedom of expression, repeatedly assessed whether "the inference at issue was 'proportionate to the legitimate aim pursued'".[18] If the overall public interest is served by disclosure, withholding the information cannot be said to be proportionate.

The most common complaint about the DIDP exceptions is that they are overly broad, an idea which is justified by comparisons against better practice laws and policies in force elsewhere. For example, the DIDP includes an exception for any information "that relates in any way to the security and stability of the Internet, including the operation of the L Root or any changes, modifications, or additions to the root zone." There is no question that ICANN should withhold information whose disclosure would pose a threat to the security and stability of the Internet. However, the current phrasing of the exception goes far beyond that, and excludes any material "that relates in any way". This could include, for example, descriptions of which departmental teams have been active in examining security issues, security gaps which have been repaired and no longer pose any active threat, etc.

The exception for "trade secrets and commercial and financial information not publicly disclosed by ICANN" is also unduly vague, and somewhat circular. Presumably, whenever financial or commercial information is subject to a request, it is being asked for because it has not been publicly disclosed. It is also unclear how this exception overlaps with the exception for "confidential business information and/or internal policies and procedures". Both of these exceptions should be deleted, and replaced with an exception for "material whose disclosure would materially harm ICANN's commercial, financial or business interests".

The DIDP exception for "drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication" also lacks a requirement for harm. While it is not uncommon for right to information systems to place draft documents off-limits while a deliberative or decision-making process is ongoing, once the process has been concluded there is no harm, and an obvious benefit, to allowing the public to see how the thought process evolved.

The exception for information requests which are "not reasonable, excessive or overly burdensome, not feasible, abusive or vexatious or made by a vexatious or querulous individual" also requires careful consideration. While exceptions for vexatious requesters are generally legitimate, experience suggests that they are also prone to abuse if their exercise is not closely watched. As a result, and because it is difficult to objectively define when a request should be considered abusive or vexatious, we recommend that the consent of the Ombudsman should be required in order to invoke this exception.

[18] See *Lingens v. Austria*, 8 July 1986, Application No. 9815/82, paras. 39-40.

The DIDP's public interest test is also problematic. Properly drafted, a public interest test operates as an exception to the exceptions, providing for the release of information where an exception is *prima facie* engaged but where disclosure is still warranted due to the overriding public interest this serves. However, ICANN's DIDP public interest test is crafted to allow for general withholding of information based on the so-called public interest even where no exception otherwise applies:

> Information that falls within any of the conditions set forth above may still be made public if ICANN determines, under the particular circumstances, that the public interest in disclosing the information outweighs the harm that may be caused by such disclosure. Further, ICANN reserves the right to deny disclosure of information under conditions not designated above if ICANN determines that the harm in disclosing the information outweighs the public interest in disclosing the information.[19]

A proper public interest override should be limited to the first sentence of this provision, allowing for additional disclosures, but not additional withholding. There are a number of reasons for this. First, a proper regime of exceptions should protect all legitimate secrecy interests, so that there is no need to provide for such discretionary extension of the regime. The overwhelming experience at the national level, where reverse public interest overrides are virtually unknown, amply demonstrates that all confidentially interests can in practice be protected effectively in this way. Second, the reverse public interest override fails to align with human rights standards, which hold that restrictions on rights are the exception and may be legitimate only if drafted narrowly and very clearly. Third, and related to the previous point, affording this sort of discretion to officials will almost inevitably lead to abuse.

One of the most important components of an effective framework for the right to information is a robust system of oversight, including a right to appeal against refusals to provide information and other violations of the rules. In most better practice governmental systems, this duty is handled by an Information Commission or Commissioner. At the national level, the independence of these institutions can be ensured through the system of checks and balances that exist in any healthy democratic environment. For example, commissioners may be appointed by the head of State from a list of nominees prepared by parliament following consultations with civil society and other key external stakeholders. RTI laws often grant commissioners security of tenure, for example by requiring the consent of a super-majority of parliamentarians or the head of the supreme court before they can be dismissed.

Obviously, there are conceptual challenges in adapting the model to the context of ICANN. Currently, appeals against refusals or other non-compliance with the DIDP are handled by the Ombudsman. However, while there are structural challenges, as well as resource constraints, which may preclude the establishment of a full time information oversight body at ICANN, one potential improvement which would allow for additional independence for the oversight system, as well as a greater measure of specialization in matters of transparency, would be to constitute an external appeals panel which, rather than sitting permanently, is retained and sits as needed. The Inter-American Development Bank has established an independent three-member panel to hear appeals, which operates on an on-call basis (i.e. rather than sitting permanently, it sits as needed when appeals are forthcoming). Importantly, panel members are

[19] Available at: www.icann.org/resources/pages/didp-2012-02-25-en.

not eligible to accept any staff, consultant or contractor positions from the IADB until three years have elapsed from the end of their service as a member of the panel. The review panel is responsible for appeals relating to information requests, and therefore represents an expert resource which the Bank can and does also use for other purposes.

Were such a review panel to be constituted, it would need to be able to exercise an appropriate set of powers, including the power to review any document, including documents claimed to be confidential, and to make orders for the disclosure of information (or, barring the ability to grant the review panel that power formally, ICANN's governing bodies should make a strong commitment to respect their decisions).

The Ombudsman's mandate regarding the DIDP should also be boosted to grant the office a stronger promotional role, including specific steps to raise public awareness about the DIDP and how it works, including by integrating understanding of transparency and the DIDP into ICANN's broader outreach efforts. Another way to facilitate requests is to make it clear to external stakeholders what sort of information ICANN. This can be done, for example, by publishing a list of the categories of information it holds and whether they are disclosed on a proactive basis, may be available via a request or are confidential.

Monitoring and evaluation are also essential to a successful right to information policy, and the Ombudsman should be tasked with tracking and reporting basic statistics on the DIDP's use, such as the number of requests received, the proportion which were denied, in whole or in part, the average time taken to respond, and so on.

Because transparency standards evolve over time, it is also important for ICANN to commit to undertaking periodic reviews of the DIDP policy, for example every five years. In its 2010 Policy on Access to Information, for example, the World Bank noted that it had reviewed its information policy in 1993, 2001 and 2005.[20]

[20] Paragraph 2.

Subtheme 2: Proactive Disclosure Policies

ICANN currently discloses its federal "lobbying" activities two ways. First, it reports such activity pursuant to the U.S. federal Lobbying Disclosure Act (LDA). Such reports are filed quarterly and are publicly available via www.house.gov and on ICANN's website. These reports reveal the general amount expended by ICANN for "lobbying," including both internal personnel and outside personnel. The LDA also requires reporting of which house of Congress and/or federal agencies were contacted by ICANN and what general issue(s) and specific legislation, if any, were discussed. Additionally, as a 501(c)(3) non-profit entity incorporated in the U.S., ICANN must abide by federal tax law with regard to its lobbying activities (must not exceed a certain threshold) and is legally obligated to disclose such interactions on its annual IRS Form 990 (reporting similarly what it reports via the LDA).

With regard to U.S. state lobbying, ICANN is presumably subject to the same reporting requirements as any other business. However, each state's reporting requirements and threshold triggers differ. A quick search of California's lobbying disclosure database does not reveal any filings made by ICANN.

In addition to hiring outside entities to engage in "lobbying," ICANN can and does hire outside "vendors" to assist ICANN externally with "education/engagement." Under federal tax law, ICANN is required in its Form 990 to disclose the identity and amounts paid to its five highest paid independent contractors. Additionally, ICANN has on its own initiative decided to report amounts paid by ICANN to all contractors in excess of $1,000,000 within a fiscal year. During the most recent fiscal year, according to ICANN, none of the vendors in the "education/engagement" category reached the $1,000,000 limit, thus the issue of disclosure of specific amounts of their work has not been triggered.

Further, as noted in an August 5, 2016 email to the CCWG-Accountability list from Xavier Calvez, ICANN's CFO, ICANN enters into vendor contracts that often include confidentiality clauses, including those requested by the vendors. According to Mr. Calvez, ICANN entered into seven contracts supporting "education/engagement" services presumably during its most recently completed fiscal year. He noted that the contractual terms prohibit ICANN from disclosing the specific amount paid to each contractor and the specific activities undertaken by the contractor on behalf of ICANN. He was able to reveal the names of each contractor and that all seven contracts were related to the IANA transition. None, according to Mr. Calvez, were engaged in "lobbying" on behalf of ICANN.

It is currently unclear if vendors must waive their confidentiality provisions in order for ICANN to report them as a "Top 5" highest paid contractor or if they trigger ICANN's self-imposed $1,000,000 reporting threshold. It is also currently unclear how the $1,000,000 threshold was arrived at and whether or not ICANN has ever reported a vendor supporting "education/engagement" activities that has triggered the threshold.

Subtheme 3: Whistleblower Protection

General Comments

WS2 Transparency appreciates that ICANN responded to a recommendation from the second Accountability and Transparency Review and retained NAVEX Global to conduct a review of ICANN's Anonymous Hotline Policy and Procedures. Overall, we feel that NAVEX produced a very solid analysis of Hotline policies and procedures and proposed appropriate recommendations for improvements.

The Staff Report notes that "ICANN is in the process of updating the Anonymous Hotline Policy and related procedures, as applicable and appropriate, to meet the recommendations and modifications proposed by the review." In general, we urge that the NAVEX recommendations be implemented by June 2017 as they address several concerns we share about the need for improvements in policies and procedures. We offer additional recommendations below.

Clarity and availability of the existing policy and employee education around it

When we initially began this examination, WS Transparency participants were keenly frustrated by not being able to readily access the Hotline policy on ICANN's public website. While we understand that ICANN employees are briefed on the Hotline policy annually, the inability of a member of the ICANN community to readily access the policy raised concerns about transparency and best practices with respect to ethics-related mechanisms.

We urge that the policy be clearly posted as "Employee Hotline Policy and Procedures" on the ICANN public website under the "Who we Are" or "Accountability and Transparency" portions as soon as possible. We further recommend inclusion of the term "whistleblower" in introductory text explaining the policy so that an ICANN community member -- who may not know that the policy is called a "Hotline Policy" – may easily locate it using "whistleblower" as the search term. For example: "The following outlines elements of ICANN's Hotline Policy and Procedures. Some organizations refer to this as "whistleblower protections." Both terms refer to an internal system for handling reports of suspected wrongdoing, mismanagement, and unethical conduct in an organization."

Related to this, the numerous hotline contact methods[21] should be listed on the public website with hyperlinks provided to the relevant page or annex of the policy. In particular, since ICANN is a global organization, we agree with the NAVEX recommendation that the international toll-free access list not be buried at the end of the Hotline policy, but referenced up front, with a hyperlink to the actual list.

We share NAVEX's concerns that the Hotline Policy and Procedures are two separate documents. Employees need a complete picture of what the policy is and how to avail themselves of it. Reading the policy document alone will not provide a potential reporter with important procedural information. Again, we urge use of the website, with appropriate hyperlinks to each document, with text explaining that the two documents are complementary and essential elements to the Hotline process.

[21] a) e-mail with email address; b) facsimile with phone number; c) web with URL; d) intranet with URL; and e) telephone via toll-free numbers both inside and outside North America

Even these basic changes, aimed at providing greater transparency concerning the Hotline policy and procedures, should help to build both employee and community trust in the process. The fact that the Hotline has received only three reports since its inception in 2008 may reflect a lack of understanding about the policy and how it works in practice. While there may be other explanations for its low use as we later explore, we believe a step in the right direction would be to provide clearer and more accessible information about the Hotline policy to via the public website.

Types of incidents reported

The ICANN Hotline policy is defined as a mechanism for employees to report "serious issues that could have a significant impact on ICANN's operations." This is definition is too limiting -- and potentially intimidating to potential reporters – and may be another reason for low use of the Hotline. For example, if an employee feels he/she is being subjected to verbal abuse or other harassment, that person may be reluctant to avail themselves of the Hotline out of concern that the abuse isn't "serious" enough because it does not involve direct financial losses to ICANN (as would suspected embezzlement or other accounting irregularities).

NAVEX recommends that ICANN drop the "serious" qualifier. We agree with that recommendation, but urge going one step further. WS2 Transparency recommends that ICANN not only clarify that employees should feel at liberty to report *all* issues and concerns related to behavior that may violate local laws and conflict with organizational standards of behavior, but also provide specific examples of such violations to guide a potential reporter. Such examples should include at minimum: verbal and sexual harassment, accounting irregularities, disregard or wrongful application of internal policies and standards of behavior, unethical conduct, abuse of authority, and reprisals for use of the Hotline process. The list should be as comprehensive as possible so an employee can feel confident that his/her concerns are legitimate, within scope, and warrant reporting.

Hotline Policy Scope

We note that the scope of the Hotline policy is limited to ICANN employees. We agree with the NAVEX report that it is appropriate to limit the scope of the Hotline policy to employees and rely on the Ombudsman to handle complaints from external stakeholders. However, NAVEX recommends that ICANN follow common practice and make the Hotline Policy and Procedures information accessible to Business Partners[22] and other "appropriate third parties as defined by ICANN" to report ethics or compliance matters.

[Question to WS2 Transparency – do you agree with NAVEX that Business Partners should have access to the Hotline and do you agree with how Business Partners is defined?]

Going back to our earlier recommendations, this underscores the importance of posting information about the Hotline Policy and Procedures on the public ICANN website and undertaking other improvements aimed at clarifying the types of incidents reported. Expanding the scope to include Business Partners therefore will necessitate additional

[22] "Business Partner is defined by NAVEX as any party that has a contracting relationship with ICANN including vendors, suppliers, temporary workers, and contractors.

language on the website explaining how Business Partners may use the Hotline and specifically limiting the types of issues they may report to ethics and compliance matters.

[Again, do we agree with this?]
We agree that an expansion of Hotline scope to include Business Partners, in turn, should be completed by revisions to the Employee Employment Policies and Procedures to include Business Partners and urge ICANN to consider the draft text proposed in the NAVEX report.

Operation of Hotline process

Internal administration of the Hotline process can be improved in several respects. The NAVEX report notes that ICANN does not utilize some type of case management system for tracking, documenting, reporting and anticipating potential problems areas. We concur that there should be some means of ensuring that all cases are documented and reported in a consistent way. This also would enable the development of more accurate statistics on Hotline reporting.

We further agree with NAVEX that such statistics should be provided to employees at least annually with a covering note from the ICANN President/CEO, followed by publication on the public website. This not only would help to inform employees that the system is being used, but also, as a complement to dropping the "serious issues" caveat, provide concrete examples of the types of issues reported. Importantly, publication of Hotline statistics would help to build employee and community trust in the Hotline system and ICANN's commitment to upholding high standards of ethical behavior.

Another measure that would help to build employee trust in the Hotline system is for ICANN to formally acknowledge receipt of the report with 24-48 hours by a secure means specified by the reporter (e.g., email, personal email, phone call, etc.). The Hotline Policy document should be revised accordingly to reflect this.

In terms of Hotline procedures, we are concerned that the Hotline Committee's determination of "urgent" and "non-urgent" is too arbitrary. This approach potentially is unfair to a beleaguered reporter who may be dealing with the debilitating effects of daily abuse. It also may delegate to "non-urgent" an underlying problem that was not appropriately addressed in the past and could quickly develop into something quite serious. The Hotline Committee should appreciate the courage involved in making a Hotline report and treat all reports with the respect for timely action that they deserve.

Addressing fear of retaliation

We have proposed several reasons why the Hotline has only received three reports since its inception in 2008: lack of clear and accessible information about Hotline Policy and Procedures; an overly narrow definition if "serious issues;" and insufficient trust in the system due to various operational shortcomings. We further propose that an employee's fear of retaliation may be an important reason by so few Hotline reports have been filed. There are several ways in which these fears can be allayed, ranging from Hotline Policy revisions to improved in-house training programs.

The Hotline policy includes language indicating that retaliation will not be tolerated. But the policy could be improved as follows: (1) it should state unequivocally that alleged retaliation

will be investigated with the same level of rigor as alleged wrongdoing; (2) it should guarantee remedy for reporters who suffer from retaliation; and (3) it should clarify that good-faith reporting of suspected wrong-doing will be protected from liability.

The NAVEX report recommends updating the Hotline Policy to define good-faith reporting and clearly state that such reporting is protected. In addition to this, we recommend that ICANN include language aimed at assuring the reporter that there are avenues for redress from possible retaliation. The language should make clear that investigations of alleged retaliation will be complete, balanced, fair and comprehensive, considering parties other than the reporter who also may be victims of such actions. Such changes will help to foster more of a "speak-up" culture and likely boost employee morale.

To complement these Policy changes, we encourage more candid discussion of retaliation in annual employee training programs. Employees should be provided examples of what constitutes retaliation for reporting suspected wrongdoing. The training also should underscore the premium placed on confidential reporting and how such confidentiality is maintained. The issue of confidentiality cannot be emphasized enough in the Policy itself as well as in posters, hand-outs and other informational documents and training programs.

Finally, in-house training should equip employees with step-by-step information on the Hotline system in practice, i.e., who in the organization literally answers the call, who will receive the report, how long it will take for the Hotline Committee to acknowledge receipt of the report (in the manner requested by the reporter), review the report, and determine the course of action.

From what little information is available to non-employees -- including WS-Transparency participants -- it has been difficult to determine the adequacy of in-house training.

Oversight and Audits

We strongly recommend that NAVEX (or a comparable and equally reputable consultancy on compliance and ethics) be retained to conduct a follow up review of the Hotline Policy and Procedures to determine the extent to which ICANN has implemented improvements recommended by NAVEX and WS2-Transparency. Owing to unusually low reporting, it is very important that the Hotline Policy and Procedures undergo regular third-party audits at least every two years. This would help to identify gaps and enable timely corrections as well as backstop other accountability mechanisms. The audit should be posted on ICANN's public website following initial review by employees.

SUMMARY OF RECOMMENDATIONS

I. The DIDP

1) **The caveat that the DIDP applies only to "operational activities" should be deleted.**
2) **The DIDP should be expanded to include clearly defined procedures for lodging requests for information, including requirements that requesters should only have to provide the details necessary to identify and deliver the information.**
3) **The DIDP should impose clear guidelines on ICANN for how to process requests, including a commitment to provide reasonable assistance to requesters who need it, particularly where they are disabled or unable to identify adequately the information they are seeking. The DIDP should commit to complying with requesters' reasonable preferences regarding the form in which they wish to access the information (for example, if it is available as either a pdf or as a doc).**
4) **The DIDP should specify that requests should receive a response "as soon as possible" and should cap timeline extensions to an additional 30 days.**
5) **The phrase "to the extent feasible, to reasonable requests" should be deleted from the provision on Responding to Information Requests.**
6) **The exception for information "that relates in any way to the security and stability of the Internet, including the operation of the L Root or any changes, modifications, or additions to the root zone" should be amended so that it only applies to information whose disclosure would be harmful to the security and stability of the Internet, including the operation of the L Root or any changes, modifications, or additions to the root zone.**
7) **The exception for "drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication" should be amended to clarify that this information should be disclosed unless it would be harmful to an ongoing deliberative or decision-making process.**
8) **The exception for information requests which are "not reasonable, excessive or overly burdensome, not feasible, abusive or vexatious or made by a vexatious or querulous individual" should be amended to require the consent of the Ombudsman before it is invoked.**
9) **The following sentence should be deleted: "Further, ICANN reserves the right to deny disclosure of information under conditions not designated above if ICANN determines that the harm in disclosing the information outweighs the public interest in disclosing the information."**
10) **ICANN should establish an external Information Oversight Panel of three members to hear appeals against DIDP refusals. The Panel should operate on an on-call basis, rather than sitting permanently. Its members should be chosen based on their expertise in relevant fields, including the right to information, and they should be prohibited from**

accepting any staff, consultant or contractor positions from ICANN until three years have elapsed from the end of their service as a member of the Panel. The Panel should be empowered to review information under request, and to order its disclosure.

11) **The Ombudsman's mandate regarding the DIDP should also be boosted to grant the office a stronger promotional role, including by integrating understanding of transparency and the DIDP into ICANN's broader outreach efforts, by publishing a list of the categories of information ICANN holds and by tracking and reporting basic statistics on the DIDP's use, such as the number of requests received, the proportion which were denied, in whole or in part, the average time taken to respond, and so on.**
12) **ICANN should commit to reviewing the DIDP every five years.**

II. Proactive Disclosure

In the interest of providing the community greater clarity with regard to how ICANN engages government stakeholders beyond the formalized GAC interactions and beyond statutory "lobbying" activities and to ensure that the ICANN community and, if necessary, the Empowered Community is fully aware of ICANN's interactions with governments, the Transparency Subgroup recommends that ICANN begin disclosing publicly the following (notwithstanding any contractual confidentiality provisions) on at least a yearly (but no more than quarterly) basis:

- **All expenditures on an itemized basis by ICANN both for outside contractors and internal personnel devoted to "political activities"[23] both in the U.S. and abroad.**
- **All identities of those engaging in such activities, both internal and external, on behalf of ICANN.**
- **The type(s) of engagement used for such activities.[24]**
- **To whom the engagement and supporting materials are targeted.**
- **The topic(s) discussed (with relative specificity).**

III. Whistleblower Protection

[23] "Political activities" is to be defined as any activity that is intended to influence or inform a government directly or indirectly on a matter of public policy.
[24] E.g., newspaper op-eds, letters, advertisements, speeches, emails, phone calls, in-person meetings, etc…

1) **The policy should be clearly posted as "Employee Hotline Policy and Procedures" on the ICANN public website under the "Who we Are" or "Accountability and Transparency" portions as soon as possible.**
2) **Related to the above, the term "whistleblower" should be included in introductory text explaining the policy so that an ICANN community member -- who may not know that the policy is called a "Hotline Policy" – may easily locate it using "whistleblower" as the search term. For example: "The following outlines elements of ICANN's Hotline Policy and Procedures. Some organizations refer to this as "whistleblower protections."**
3) **The definition of incidents reported should be broadened from "serious issues" to encourage the report of *all* issues and concerns related to behavior that may violate local laws and conflict with organizational standards of behavior. Furthermore, the policy should provide specific examples of such violations to guide a potential reporter.**
4) **[Scope of Policy – I received one comment opposing broadening the scope to include "Business Partners." We need a WS2-Transparency consensus on whether to support/oppose the NAVEX recommendation to broaden scope to include Business Partners and revise the text accordingly.]**
5) **ICANN need to improve internal administration of the Hotline process by employing case management software to better enable tracking, documenting, reporting and anticipating potential problem areas.**
6) **ICANN should regularly provide employees with data about use of the Hotline, that details not only the frequency of use but also the types of incidents reported.**
7) **ICANN should not prioritize receipt of reports as "urgent" and "non-urgent," but treat every report as a priority warranting formal acknowledgment of receipt of a report within 48 hours at the latest.**
8) **ICANN needs to more effectively address potential fear of retaliation against the reporter by stating unequivocally that alleged retaliation will be investigated with the same level of rigor as alleged wrongdoing. ICANN should also guarantee remedy for reporters who suffer from retaliation as well as clarify that good-faith reporting of suspected wrong-doing will be protected from liability.**
9) **ICANN's Hotline Policy and Procedures should undergo a third-party audit least every two years to help identify gaps and enable timely corrections. The audit, in turn, should be posted on the public website.**

Annexes

Resources