GAC Public Safety Working Group (PWSG) Public Comments to "2013 RAA WHOIS Accuracy Specification Review"

The PSWG believes the current 2013 Registrar Accreditation Agreement (RAA) WHOIS Specification is serving its intended purpose to enhance the accuracy of the WHOIS data and the requirements should be maintained. If greater efficiencies or alternative models/methods can be used to achieve the goal of accurate WHOIS, the GAC PSWG would support such efforts. Upon review of comments submitted by ICANN and the Registrar Stakeholder Group, the GAC PSWG offers the following comments.

ICANN Staff Input

The PSWG concurs with the following ICANN Staff recommendations:

1. Insert clear definitions of verification and validation into the WHOIS Specification in Section 1:
   "Verification: The process by which a registrar confirms or corrects the accuracy of Whois data by contacting and receiving an affirmative response from the Registered Name Holder.

   Validation: The process by which a registrar ensures that the format of Whois data is consistent with standards. "

2. Ensure the WHOIS Specification; Section 1, is explicit in stating data needs be verified/validated before registration.
3. The WHOIS Specification, Section 5, should require verification, in addition to validation, where a domain name was suspended due to inaccurate Whois data, since the inaccurate data presumably passed validation checks already.

Registrar Stakeholder Group Input

The PSWG has the following questions and/or recommendations regarding Registrar Stakeholder Group Input:

1. Define "alternative, non-UPU formatting sources" and why the UPU templates are not acceptable. The use of multiple and possibly non-standard formats could be a problem because ICANN's WHOIS Online Accuracy Reporting System cannot function unless there are agreed-to data format standards.
2. Registrar Stakeholder Group requested in several sections of the WHOIS Specification to increase response time from 15 days to 45 days. Why is it necessary to extend the Registered Name Holder response time from 15 days to 45 days?
3. The Registrar Stakeholder Group requested inclusion of the terms "substantial" and "substantiated" in several sections of the WHOIS Specification. Both terms should be explicitly defined. After they have been defined, there should be a determination if such language is warranted or necessary for inclusion in the WHOIS Specification.

GAC PSWG Input

The PSWG recommends the WHOIS Specification remain in force with its current requirements, Nevertheless, the PSWG welcomes continued dialogue with the Registrar Stakeholder Group to further clarify and consult on requested Registrar Stakeholder Group edits to the WHOIS Specification.

The PSWG expresses particular concern to the proposal for extending the response window to 45 days. UK Law enforcement agencies commented that such a relaxed time frame would make it easier for organised crime groups to both register domain resources and prolong 'uptime' of criminal infrastructure. Extended comments from UK LEA regarding this issue are contained in Annex 'A'.

In addition, the PSWG recommends, per the 2013 Registrar Accreditation Agreement (RAA) that the Cross-Validation requirement be completed and incorporated into the WHOIS Specification by the end of 2015. ICANN and the Registrar Stakeholder Group had resolved to have the Cross-Validation RAA requirement implemented within six (6) months of the RAA in January 2014.

Annex A - UK Law Enforcement Comments on WHOIS Specification Review

Post ICANN 2009 to 2013 RAA contractual migration, ICANN compliance has reported and increase of registrar complaints related to Whois inaccuracy as rising from 57.9 percent in 2013 to 74.3 percent in 2014. For the first quarter of 2015, Whois inaccuracy comprised 74.0 percent of complaints.

Against the latest ICANN contractual compliance figures UK law enforcement welcomes the commitment of ICANN accredited registrars in validating and verifying WHOIS registrant data to an increased standard of due diligence and ownership with a continued need to maintain such a threshold of validation and verification.

Proposed Registrar changes to allow WHOIS registrant data to be validated and verified over a 45 day period as opposed to a current 15 day period are a cause for concern for UK law enforcement and may have an adverse impact against the current high compliance standards in terms of response times which in law enforcement cases must continue to be current (15 days or under) to prevent and detect malicious WHOIS registration.

UK law enforcement feel that a more relaxed and lengthier period of 45 working days to validate becomes more attractive to organised crime in the registration and also the long term use of a domain name for malicious purpose.

Law enforcement priorities in Internet policy concentrate on reducing the “uptime” of a suspicious domain name as do other interested parties in making the Internet a safer place, for example the Anti Phishing Working Group (APWG) in reducing the uptime of phishing domains to prevent loss to victims.

The suggestion of increasing the response window from 15 days to 45 days is a very concerning recommendation. 15 days is already quite a generous amount of time for a registrant to verify their contact information. Where the verification has been prompted by a request from law enforcement, any increase in the time window would have a potential knock on effect for investigation lengths and also potentially expose more members of the public to becoming victims of crime. The increase in investigation time could mean that other data that might be subsequently requested may no longer be available due to short retention times for certain data and therefore could have a significantly negative impact on the ability to identify and prosecute offenders. Before any extension of the 15 day window I would like to understand why 45 days is being suggested and why 15 days is not currently enough. From a public safety perspective I would prefer to the see the window reduce rather than increase.

Such a relaxed time frame would make it easier for organised to crime to both register domain resources and also afford them the luxury of between 1-2 months use before real examination by Registrars.

Internet governance efforts by Industry, most notably the ICANN 2013 RAA agreement have seen a paradigm shift in Industry in the way a domain name is viewed as “suspicious” before being validated as “good” within the 15 day period of review.

UK law enforcement’s view is that a 45 day period would revert Industry back to a culture of viewing domains “good” until they are proven “bad” therefore allowing crime to propagate and increase harm online.

The onus would therefore fall back on to LE and Hosting providers to carry our crime prevention on a more reactive scale in an environment where the average uptime of a domain involved in a cyber crime activity is seen as days and not weeks or months. Such a move would defeat the object of a current working and successful RAA model.

Associated to this success the pre RAA 2013 LE / Registrar negotiations saw the creation of an agreed and adopted "5 C's" validation and verification scoring model allowing Registrars to effectively credit score core fields of registrant WHOIS data (address, phone, email etc) to a "reasonable" level taking into account the global market for domain name purchases and the wide variation in registrant WHOIS data.

UK law enforcements puts forward the need to continue to use this approach to create a manageable compliance response to new and existing domain name registrations with the associated 15 day window still seem as sufficient to allow validation and verification issues to be corrected to both prevent malicious registrations and also to negate and prevent domain suspensions of innocent holders subject to incorrect WHOIS entries.

UK law enforcement request that this process continues and for Registrars to strike a balance between 5C validation and normal trade, working together with an ICANN compliance function that has Industry oversight to identify the minority of registrars who may currently not validate and verify WHOIS for example thorough :

-PSWG Case Study evidence of abuse and RAA 2013 breaches

-WHOIS accuracy studies

-Proposals for "holding periods" for domain names / strings suspected as used in DGA cyber crime activity

-Flagged issues such as domains registered using stolen accurate data

-Identification of consistent registrar of greater compliance interest not adhering to RAA 2013 standards

UK law enforcement are keen to continue to work proactively with ICANN, Registrars, and global law enforcement to target the consistent offending registrars who are attractive to organised crime through LE submissions of abuse and case studies to further highlight the problem offenders in the market and support the registrars who continue to deny organised crime the ability to register Internet resources for criminal misuse.