

I. **Parallel/Overlapping Recommendations of Task Force 3 Majority and Registrar's Minority Reports**

A. Contract Compliance:

1. TF3: 1./2. ICANN should work with all relevant parties to continue to create its ongoing compliance program to ensure that contractual parties are meeting the WHOIS-related provisions of the present agreements.

(full text identical).

2. Minority Report: c.b.4. ICANN should work with all relevant parties to continue to create its ongoing compliance program to ensure that contractual parties are meeting the WHOIS-related provisions of the present agreements. (full text identical).

B. New Whois Data Elements

1. TF3: 5. ICANN should also consider including the “last verified date” and “method of verification” as Whois data elements as recommended by the Security and Stability Advisory Committee.

2. Minority Report: c.a.i. Whois data must contain a “Last Verified Date” that reflects the last point in time at which the information was known to contain valid data. It must also contain a reference to the data verification process.

c.a.ii. A Whois service must discourage the harvesting and mining of its data.

c.a.iii. Whois services must provide mechanisms to protect the privacy of registrants.

c.a.iv. Whois records known to be false or inaccurate must be frozen or held until they can be updated or removed.

c.a.v. Whois records that have information that can not be validated may be frozen or held until it can be verified.

c.a.vi. A standard format for Whois data must be developed.

c.a.vii. A publicly available list of publicly available Whois servers must be available using a widely known and available resource.

c.a.viii. A Whois service that supports searching in the current architecture of distributed indices and separated registry and registrar services must be developed.¹

¹ These recommendations come from the Whois Recommendation of the Security and Stability Advisory Committee, at <http://www.icann.org/committees/security/sac003.htm>

- C. Identification of Contact Point for Receipt of Whois Data Inaccuracy Complaints
1. TF3: 6(a). Plans to improve contract compliance and Whois accuracy state specific steps, including: Identification and public disclosure of a designated contact point for receiving and acting upon reports of false Whois data.
 2. Minority Report: a.a.i. Registrars must identify and disclose a designated public contact point responsible for receiving and acting upon complaints received via the mandatory Whois Data Problem Reporting System (WDPRS) and related whois record data accuracy issues. ICANN should amalgamate and publish this list on their website.
- D. Training Registrar Employees on Whois Data Accuracy Requirements
1. TF3: 6(b). Steps should include plans to work with ICANN to train employees and agents regarding the Whois data accuracy requirements.
 2. Minority Report: a.a.ii. Registrar should certify that this contact point has been trained on Whois Data Accuracy policy requirements.
- E. Steps to Screen Registrant Data for Inaccuracy
1. TF3: 6(c). Steps should include taking reasonable steps to screen submitted contact data for falsity, including use of automated screening mechanisms, manual checking, spot-checking, and other verification techniques for submitted data.
 2. Minority Report: a.c. Registrars should take reasonable steps to prevent Registrants from supplying inaccurate data at the time of registration.
c.b.i. Registrars must verify Whois data in a timely fashion when specific data accuracy issues are brought to their attention.

II. Other Possible Recommendations

- A. Targeting “Bad Actor” Registrants
1. Responsive to Bruce Tonkin’s suggestion (email of Aug. 18, 2004 item (b)) for dealing with bad actors, those who purposefully, and fraudulently, register domain names, and “game” the system by exploiting delays in the domain name system’s ability to respond to fraud allegations (e.g., 15-day window for updating false contact data).
 2. Such a system would require registrars to place on hold or remove domain name registrations, supported by false contact data, when presented with reasonable evidence that the domain name is being used to infringe intellectual property rights, or commit other illegal acts.
 3. Such a system would require designating a point of contact for receipt of notices of claimed infringement. This is different from the Minority

Report Recommendation a.a.i. (above) which suggests only a contact point for receipt of WDPRS complaints. The MOU requires ICANN to “[c]ontinue to assess the operation of the Whois databases and to implement measures to secure improved accuracy of Whois data.” <http://www.icann.org/general/amend6-jpamou-17sep03.htm>. The WDPRS is one means of meeting this goal but does not constitute the entire effort.

B. Graduated Sanctions

1. Task Force 3 Majority Recommendation 12: “ICANN should develop and implement a graduated scale of sanctions that can be applied against those who are not in compliance with their contractual obligations or otherwise violating the contractual rights under these agreements.
2. Was not agreed to by the Minority Report: “. . . the requirement to admit liability and submit to a managed remediation plan in the event that a registrar is non-compliant with some or all of their Whois related obligations is an unworkable aspect of this document.” <http://www.gnso.icann.org/issues/whois-privacy/TF3PreliminaryWithRCMR1.pdf>, at page 18.
3. Graduated Sanctions are part of ICANN’s compliance program as outlined in the revised budget: “The elements of the initial [compliance] program will consist of. . . Implementing a planned escalation of actions and cures, including legal and specific performance remedies, in order to correct ongoing harm and to ensure legitimacy for the compliance function.” <http://www.icann.org/financials/budget-fy04-05-21jul04.html>.

C. Task Force 3 Recommendations for Registrar Duties

1. TF3 Recommendations 8-10
 - a. Rec. 8 - Verification of two out of three contact points. If no contact point is accurate, place domain name on hold. If one contact point is inaccurate, place domain name on hold for 15 days to allow registrant to correct information. Domain name should be cancelled if registrant fails to correct data.
 - b. Rec. 9 - Domain name can be reconnected for a fee charged by the Registrar. Registrar shall have a duty to verify the accuracy of data for reconnected domain names.
 - c. Rec. 10 - If a domain name is cancelled or placed on hold for inaccurate contact data, then all other domain names with that contact data should likewise be cancelled or placed on hold.
2. Minority Report Recommendations c.b.i - c.b.iii. Similar to Majority Report Recommendations 8-10, but require no affirmative steps by Registrars. Instead, registrars are only required to act when “specific data accuracy issues are brought to their attention.”