FIRST™
Improving Security Together

15 March 2018

Dear ICANN, dear Members of the Governmental Advisory Committee,

With great interest, FIRST and our community have been following recent discussion around the WHOIS service in light of the new European General Data Protection Regulation (GDPR).

For security teams, our constituency, WHOIS information has proven an invaluable tool in investigating and responding to security teams. The use cases for the data are varied, and to help contribute to the discussion, FIRST will start publishing use cases from our membership in the next few weeks via our website, https://www.first.org. A select number of ways in which WHOIS data is used by our membership include:

- To inform the owner of an internet service of a security incident affecting them;
- To identify multiple domain names being registered to an individual malicious actor.

FIRST also believes privacy is an important goal, and we appreciate the ongoing discussion around how WHOIS data can be maintained and exposed in a more privacy sensitive way. We also acknowledge the security uses of WHOIS data support privacy of users in a meaningful and important way.

In general, FIRST is supportive of a mechanism for tiered access to non-public WHOIS data. It provides mechanisms for those with a need to access, to continue to still use the information, while limiting the privacy risk to individual user information. However, we have several concerns which should be addressed:

- Current ICANN process places a strong burden on the Governmental Advisory Committee to provide input to the determination of which user groups are eligible to the accreditation program. Security teams are not always, nor typically, accredited by their national government.

  An incident responder within private sector, academia, may have responsibility over multiple client or organization networks, and need access to WHOIS data to investigate malicious activity. Even security teams with national responsibility are not always government entities, or even endorsed by their national government. The FIRST membership is an organization of over 400 member security teams across 86 countries, and restricting access to organizations endorsed by their national government could significantly hamper the ability of our community to partner on responding to security incidents.

- We recognize ccTLD operators are not covered by current ICANN guidance, which focuses on the gTLD operators, where contractual provisions apply. While this means ccTLD operators may implement compliance in different ways, we encourage ICANN to engage in outreach, tool building and some level of voluntary coordination across the ccTLD operator network as well. Having uniformity in approach between gTLD and ccTLD implementations, including ensuring accreditation of access is uniform across registry operators will be essential in ensuring continued usability of WHOIS.

We recognize the complexity of the challenge ahead, and FIRST welcomes any opportunity to contribute to the design and implementation of any protocol or accreditation service. WHOIS is an indispensable service for our membership, and we are committed to supporting ICANN and the Governmental Advisory Committee in ensuring its continued usability.

Best regards,

Schreck Th

Thomas Schreck

Chair, Forum of Incident Response and Security Teams

Founded in 1990, the Forum of Incident Response and Security Teams (FIRST) consists of internet emergency response teams from more than 360 corporations, government bodies, universities and other institutions across 78 countries in the Americas, Asia, Europe, Africa, and Oceania. It promotes cooperation among computer security incident response teams. For more information, visit: https://www.first.org.