United States Government Comments to ICANN re.
Article 29 Data Protection Working Party Guidance

The United States Government (USG) thanks ICANN for the opportunity to respond to the guidance provided by the Article 29 Data Protection Working Party (WP29). The WP29 guidance is valuable in evaluating ICANN's proposed GDPR compliance model and improving it to ensure GDPR compliance is achieved in a manner that maintains the current WHOIS requirements to the greatest extent possible. While the WP29 guidance is helpful and points to several areas in which the model can be improved, the USG is concerned with other aspects of the guidance which appear to rely upon an incomplete view of ICANN's mandate and the purposes of the WHOIS. The USG is also concerned the WP29 did not address the issue of a temporary moratorium on enforcement.

The Criticality of WHOIS Access for Legitimate Purposes

The USG remains concerned that the inaccessibility of WHOIS information presents a serious threat to the stability and security of the Domain Name System (DNS). We are concerned that the WP29 guidance does not recognize the necessary balance between privacy and the legitimate purposes for data processing. Regrettably, this guidance will likely empower companies to provide less WHOIS information (and perhaps none at all) even though it is not necessary under EU law. The GDPR recognizes the importance of balancing privacy with the processing of and access to data for legitimate purposes. While the USG agrees that data privacy is of critical importance, we also believe that public safety and rights protection are equally critical.

ICANN's Mission and Mandate

The USG is concerned that the WP29 guidance misinterprets and misrepresents the ICANN mission and mandate, which WP29 then uses as the basis for guiding ICANN on its purpose specifications. Specifically, the WP29 guidance cautions ICANN to define its purpose in a manner that is consistent with its mission and mandate and not to align itself with the interests of third parties, but then refers to an incomplete articulation of ICANN's mandate and mission.

ICANN's Bylaws make clear that ICANN's mandate is to "ensure the stable and *secure* operation of the internet's unique identifier systems" [emphasis added].[1] Further, ICANN's Bylaws include a commitment to preserve and enhance "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet."[2] Finally, ICANN's commitments emphasize that it must "adequately address" issues related to "consumer protection, security, stability, resiliency [and] malicious abuse. . . ."[3] Regarding registration data specifically, ICANN's Bylaws recognize that WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust."[4]

[1] ICANN Bylaws Article One, Section 1.1, Mission.
[2] ICANN Bylaws Section 1.2 (a) Commitments and Core Values.
[3] *See* ICANN Bylaws Section 4.6 (d), Specific Reviews, Competition, Consumer Trust, and Consumer Choice Review.
[4] ICANN Bylaws, Registration Directory Services Review, §4.6(e).

In addition, those Bylaws require ICANN to use commercially reasonable efforts to enforce its policies relating to the Registration Directory Service, while exploring structural changes to improve accuracy and access to generic top-level domain registration data, as well as considering safeguards for protecting such data. In fact, to the extent law enforcement, cyber security, and intellectual property rights professionals use publicly available WHOIS data to detect and combat threats to the infrastructure of the DNS, the collection and disclosure of this data to these groups is essential to ICANN's core mandate: the security of the DNS and the Internet. We note that these legitimate interests are consistent with the recitals to the GDPR, which permit processing of personal data for:

1) "preventing fraud";

2) "ensuring network and information security," including the ability of a network or information system to resist "unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services;" and,

3) reporting possible "criminal acts or threats to public security" to authorities.[5]

The USG asks that ICANN bring an accurate description of ICANN's mandate and mission to the attention of the WP29. This has tremendous bearing on ICANN's purposes in data processing and corrects the record that somehow ICANN is inappropriately aligning itself with interests of third parties.

Publication of Email

As noted by governments in the ICANN61 Governmental Advisory Committee (GAC) communique,[6] it is questionable whether the exclusion of email addresses in the public WHOIS is required to be compliant with GDPR. While the WP29 guidance welcomes ICANN's proposal for alternative contact methods, such as anonymized email, etc., the USG remains concerned that this approach is over-compliant with GDPR. It would be helpful if the WP29 could address the GAC's concern that the proposal not to publish the registrant email addresses may not be proportionate in view of the significant negative impact on law enforcement, cybersecurity, and intellectual property rights protection. It is understood that email *could* include personally identifiable information, but there is nothing requiring the registrant to elect to provide an email that is not anonymous in that regard. Moreover, the registrant's email address is often the most important data point for law enforcement, consumer protection, cybersecurity, and IP rights protection. The email address is likely to be more accurate than other WHOIs information - particularly for bad actors - since registrars must validate the email address and a working email address is necessary for the registrar and registrant to

[5] *See GDPR* Recitals 47, 49 and 50.
[6] *See* https://gac.icann.org/contentMigrated/icann61-gac-communique

communicate about payments, expirations, etc. Keeping the registrant email address in public WHOIS allows: (i) a broad array of threats to be recognized and addressed quickly, and (ii) damage from such threats to be contained, particularly where the abusive/illegal activity may be generated from a variety of different domain names. Having the registrant's email address in public WHOIS also protects registrants themselves. As noted in a recent cyber security blog, "the overwhelming majority of phishing is performed with the help of compromised domains, and the primary method for cleaning up those compromises is using WHOIS data to contact the victim…"[7]

Security

The USG welcomes the WP29 commitment to security of data, however we are concerned that the guidance provided misses a fundamental point. That is, accreditation is the threshold process by which to determine access and ensure the appropriate level of access. Whitelisting, as cited by WP29, is one technical means by which to then provide the actual access to WHOIS information. The ICANN proposed model proposes a system in which accreditation is foundational and the technical means (whether it is credentialing, whitelisting, passwords, etc.) are yet to be identified. That being said, whitelisting should not be taken off the table. Whatever technical means is ultimately employed will need to address security, but we think it is premature for the WP29 to make that technical determination when there is as yet no specific system in place to evaluate.

Enforcement Moratorium

The USG, like ICANN, believes that an enforcement moratorium is a necessity as ICANN and its contracted parties work to implement a GDPR compliance plan and that the users of WHOIS also have the time to develop compliant accreditation system(s). National Governments also need time to develop mechanisms by which to identify government users, such as law enforcement, which are not users targeted by the GDPR but nonetheless are forced to comply with this regulation. In order to ensure that critical legitimate purposes are not hindered in their activities, it is imperative that a limited short-term moratorium on GDPR enforcement is considered for the WHOIS and its legitimate users.

[7] *See* blog by world-renowned cybersecurity expert Brian Krebs about the potential impact of the GDPR on security: https://krebsonsecurity.com/2018/02/new-eu-privacy-law-may-weaken-security/#more-42552.