From the desk of
Jonathan Matkowsky, VP – IP & Brand Security

Writer's Direct Cell: (206) 556-0118

VIA EMAIL <goran.marby@icann.org>, <cherine.chalaby@icann.org>

Mr. Göran Marby
ICANN President and CEO

Mr. Cherine Chalaby
Chair
ICANN Board

April 20, 2018

Follow-up Request for Adequate Assurances Relating to WHOIS and GDPR

Dear Messrs. Marby and Chalaby:

This is a follow-up on our request for adequate assurances relating to WHOIS and GDPR.

With respect to the draft IPC/BC Accreditation and Access Model for Non-Public Whois Data, RiskIQ notes that the fact that security interests are being represented by some organizations whose representatives happen to be SSAC members is not the same thing as saying that SSAC members are representing security interests in the community discussion.

SSAC is responsible under the Bylaws to make policy recommendations to the ICANN Community and Board relating to, amongst other things, the security of the Internet's naming system.[1] This includes registration matters pertaining to WHOIS services (as reflected on SSAC's homepage). **SSAC should immediately weigh in for the ICANN Community, and so advise the Board to approve a Temporary Policy with a sense of urgency to preserve the security of the Internet's name system by mitigating expected harm from a fragmented WHOIS leading up to the GDPR enforcement deadline**. Because there is no guarantee that ICANN will receive a reprieve from enforcement of GDPR, the Board needs to swiftly approve a Temporary Policy to restore ICANN's Mission.

As background, Registrars must comply with and implement all specifications or policies established by the Board on a temporary basis, if adopted by the Board by at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are

[1] ICANN Bylaws, § 12.2(b).

justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registrar Services, Registry Services or the DNS or the Internet.[2]

Under the ICANN Bylaws, the Chair of the Board or the President or at the request of one-quarter of the Directors may call for a Special meeting made by the Secretary.[3] We strongly recommend that SSAC weigh in to this community discussion, and advise whether it agrees that the Board should utilize this provision to establish an enforceable Temporary Policy to preserve the security of the Internet's name system by mitigating harm from a fragmented WHOIS.

In our view, such a Temporary Policy would cover three general areas: (1) the criteria for accessing the non-public data set for security or stability of the Internet's naming system; (2) IP whitelisting security parameters and rate limiting restrictions associated with such access; and (3) the format for contracted parties to use for the WHOIS output.

All three areas must be narrowly tailored as feasible for purposes of preserving the security or stability of the Internet's name system[4] until a community PDP will endeavor to formulate a permanent compliance model for WHOIS, or its replacement, within what will inevitably turn into a one-year temporary policy period.

With respect to (1) the criteria for accessing the non-public data set or accreditation process under the Temporary Policy, **SSAC should advise the ICANN Board to instruct the ICANN org to immediately assemble an expert working group with representatives from the security community such as FIRST, M3AAWG, and APWG to draft the criteria for accessing the non-public WHOIS contact information that can be incorporated into the Temporary Policy**. In this regard, RiskIQ's recommendation is consistent in all material respects with the recent recommendations from the Forum of Incident Response and Security Teams (FIRST) on April 19, the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) on April 13, as well as from APWG on April 5.[5] Such correspondence is attached hereto for your reference, but summarized immediately below.

---

[2] 2013 RAA, Consensus and Temporary Policies Specification § 2. In establishing any Temporary Policy, the Board must state the period of time for which the Temporary Policy is adopted. ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the Temporary Policy and why the Board believes such Temporary Policy should receive the consensus support of Internet stakeholders. If the period of time for which the Temporary Policy is adopted exceeds 90 days, the Board shall reaffirm its temporary adoption every 90 days for a total period not to exceed one year.

[3] ICANN Bylaws, § 7.15.

[4] 2013 RAA, Consensus and Temporary Policies Specification § 2.1.

[5] In the interest of disclosure, RiskIQ is a member of The FIRST, APWG, and M3AAWG.

From APWG:

"*We recommend that the ICANN Board pass a Temporary Policy to make an accreditation plan a reality as soon as practical.*"
...

"APWG is willing to help craft specific accreditation procedures, including what kinds of documentation and bona fides should be required of applicants, specifically security actors and researchers."

From the FIRST:

"FIRST encourages the ICANN Board to instruct ICANN org to move forward with a sense of urgency to implement an accreditation plan...We support the previous recommendations...to establish a community group, including the antiabuse, and incident response communities, to facilitate the creation of an accreditation model for qualified applicants from the security community. FIRST welcomes any opportunity to participate in such an expert task force to draft those requirements…"

From M3AAWG:

"We agree that an expert group from the Anti-Abuse community including APWG, FIRST and M3AAWG should be created to facilitate the certification of qualified applicants from the security field."

RiskIQ believes that if SSAC advises the Board to instruct the ICANN org to act immediately in this regard, an expert security working group can quickly align the criteria for accessing the non-public registrant contact information under a Temporary Policy with the checklist made available from the Singapore Accreditation Council (SAC), the national authority for the independent accreditation of conformity assessment bodies in Singapore. SAC has a publicly available Assessment Checklist (ISO/IEC 17065) from September 2013 available to work from for download here.

With respect to (2) IP whitelisting security parameters and rate limiting restrictions, RiskIQ, like the FIRST, M3AAWG, and APWG, supports the proposal to enforce use of an interim IP Whitelist for access to the registrant contact information in WHOIS data for anti-abuse, threat intelligence, and incident response while a more mature accreditation plan is being implemented. As The FIRST stated:

"*Therefore, we specifically recommend that the ICANN org create a special task force of security experts to sketch out how the IP-based access could be implemented in a manner that mitigates the WP29 concerns while still protecting the security of the unique identifiers during any interim period to avoid a blackout in May.*"

In our view, temporary disruption of continuous access for security purposes such as incident response, abuse reporting, threat intelligence and anti-abuse is otherwise likely to impair the technical and organizational security measures that are actually being relied on currently to ensure a reasonable level of security.[6] Such security measures include public WHOIS. Similar to APWG, we believe **accredited temporary access to registrant contact information should not be rate-limited except to prevent system overload** to ensure that the temporary tiered-access works for its intended purpose.

With respect to the (3) format for contracted parties to use for the WHOIS output, RiskIQ believes it is practical at this point to take a two-tiered approach: records for newly registered domains versus what to do with the existing records. For newly registered organizational domains, it is critical to instruct the contracted parties in the Temporary Policy not to collect personal data that is not required to be collected and that otherwise should remain in the public data set from a security perspective. A requirement that the registrant org email be in the format of "Admin" or "Manager" [at] second level domain would avoid GDPR concerns all together, and keep the registrant org email address for newly registered domains in the public data set for security, which serves ICANN's Mission. Without this information in the public data set, organizations have less visibility into their own organization's digital footprint. If an organization cannot see which domains were registered from its corporate accounts, then these overlooked sites will not end up having vulnerability scanning, and makes them more susceptible to targeted exploits.

With respect to existing WHOIS records for organisational domains, a Temporary Policy should allow the contracted parties to obfuscate or mask only the local part of the registrant organizational email address in the public data set to the extent they deem it necessary or advisable from a privacy perspective. The local part is the only part of the organizational email address that poses any possible risk of containing information relating to a natural data subject that arguably should not have been collected. There should be a conspicuous notice that goes out allowing registrant organizations to opt-out from masking the local part of the organizational email in existing records, explaining the upside and downside from a privacy and security perspective.

We want to close by taking this opportunity to express our concern that by not getting adequate consent from individual registrants to mask their existing data from public WHOIS, **GDPR is being used to unilaterally change the security environment under which registrants agreed to process their data to begin with**. Individual registrants should be given the opportunity to opt-in to continuing to disclose their information in public WHOIS, as to mask it without their permission changes the technical and organisational measures used to ensure a level of security appropriate to the risk. Many that have registered domains did so subject to the understanding that public WHOIS is in place, and available for the threat intelligence, anti-abuse and incident response. This transparency and open directory is part of the checks and balances used to ensure the security of domains because the contracted parties can always be notified using this public

[6] This concept of taking WHOIS into account as a technical and organisational security measure is referenced in CIRCL's TR-53. CIRCL is the CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg.

WHOIS directory and services that they have been compromised, and the registrants could expect public WHOIS contact information to be leveraged to contact them if their domains have been compromised. The current threat landscape is premised on this information being available publicly and used to mitigate threats.

Sincerely,

cc: SSAC (ssac-staff@icann.org); accred-model@icann.org

19 April 2018

We also wanted to repeat the **criticality of including valid organizational contact information in the public WHOIS** data set for at least newly registered organizational domains. There is no reason why personal data of individual name holders should continue to be collected if it unnecessarily limits what is displayed in the public WHOIS. Therefore, a temporary policy should also address the formatting requirement of the organizational email address to allow a valid “admin” or “manager” user at a particular domain (or possibly an anonymized or pseudonymous proxy address) .

There is no true privacy without security. We strongly believe one of the key criteria that should be met is that registrars should be transparent to users on which data is exposed, and to whom. Having a clear, universal message to users around how their data is stored, and presented to both the security communities, and the internet at large, is key to making expectations clear.

We read with great interest the proposal of the Anti-Phishing Working Group, dated April 5th of 2018. FIRST is eager to work with its industry peers, including M3AAWG and APWG, with whom we are already in contact, to help define an accreditation model that will allow our members, and the wider security community to gain access to WHOIS data.

Best regards,

Thomas Schreck	Maarten Van Horenbeeck	Serge Droz	Aaron Kaplan
Chair	Board Member	Board Member	Board Member
thomas@first.org	maarten@first.org	serge@first.org	aaron@first.org

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.

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

To: ICANN (Internet Corporation for Assigned Names and Numbers)
VIA Email: gdpr@icann.org, goran.marby@icann.org and accred-model@icann.org

From: Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

Date: April 13, 2018
Subject: WHOIS Tiered Access and Accreditation Program: Comments from M3AAWG

Dear Mr. Göran Marby CEO, ICANN:

We agree with the Anti-Phishing Working Group's (APWG) comments dated April 5, 2018 that the anti-abuse community needs the ICANN Board to pass a Temporary Policy to make an accreditation plan a reality, directing the participation of the registry operators and registrars.

We agree that an expert group from the Anti-Abuse community including APWG, FIRST and M3AAWG should be created to facilitate the certification of qualified applicants from the security field.

We support a short-term plan discussed on the April 6th conference call offering tiered WHOIS access to authorized IP addresses until a more sophisticated mechanism can be a further developed with details for accredited access.

Sincerely,
Jerry Upton, Executive Director
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 https://www.m3aawg.org

Unifying the Global Response to Cybercrime

April 5, 2018

Mr. Göran Marby
CEO, ICANN

Dear Mr. Marby:

ICANN Org and community members have proposed an accreditation program to provide tiered access to non-public WHOIS data by qualified parties. The Anti-Phishing Working Group (APWG) supports the creation of such a program and is interested in helping it reach fruition quickly. In this document we comment about the requirements for the program. We also propose a short-term technical execution that we believe can be implemented in mid-2018, with a longer-term and more sophisticated access system to be created following that. Our comments focus on sensible ways to provide GDPR-compliant access for qualified parties, and prevent fragmentation of the WHOIS system. We recommend that the ICANN Board pass a Temporary Policy to make an accreditation plan a reality as soon as practical.

APWG is also willing to act as an expert group to facilitate the certification of qualified applicants from the security field. APWG envisions itself as one, non-exclusive body that can do so, and hopes that other bodies will step forward to serve various communities who have legitimate needs to access non-public domain registration data.

We support the contours of the "Model 1.3" accreditation plan (the "Cannoli Model"') proposed by ICANN's Intellectual Property Constituency and its Business Constituency. That plan lays out a rational framework, and we support it with the modifications described below.

APWG will continue to participate in community discussions of the accreditation plan. Greg Aaron and Rod Rasmussen, the co-chairs of APWG's Internet Policy Committee, will coordinate the APWG's work on this important subject. Thank you for your attention and we look forward to your support.

Sincerely yours,

--Peter Cassidy
Secretary-General, APWG

cc: gdpr@icann.org, John Jeffrey (jj@icann.org), Brian Winterfeldt (brian@Winterfeldt.law)

WHOIS Tiered Access and Accreditation Program:
Proposal and Comments from the Anti-Phishing Working Group (APWG)

version 1.0, 5 April 2018

Authors:
Greg Aaron (iThreat Cyber Group; APWG Senior Research Fellow)
Pat Cain (Resident Research Fellow; APWG Board of Directors)
Peter Cassidy (APWG Secretary-General; APWG Board of Directors)
Dave Jevans (Chairman, APWG Board of Directors)
Rod Rasmussen (R2Cyber; Co-Chair APWG Internet Policy Committee)

CONTENTS

EXECUTIVE SUMMARY

ICANN Org has proposed an accreditation program to provide tiered access to non-public WHOIS data.[1] This program would involve "codes of conduct which would establish the standardized criteria, limitations, and responsibilities for granting access to non-public WHOIS data to the accredited parties. Selection of the accredited parties could be facilitated by designated expert groups."

In this document we comment about the overall requirements for any ICANN accreditation program. APWG is also willing to act as an expert group to facilitate the certification of qualified applicants from the security field.

We recommend that the ICANN Board pass a Temporary Policy to make an accreditation plan a reality, directing the participation of the registry operators and registrars. Below (we propose a technical execution scheme that we believe will be practical to implement in mid-2018, thereby enabling access for authorized parties while a longer-term program is developed. (See "Proposed Operating Model" on pages 10-12.)

We support the contours of the "Model 1.3" accreditation plan (the "Cannoli Model") proposed by ICANN's Intellectual Property Constituency and Business Constituency.[2] That plan lays out a rational framework, and we support it with the modifications described below.

The below document has been reviewed by the APWG Board of Directors.

[1] As of this writing, ICANN Org's "Proposed Interim Model for GDPR Compliance" or "Calzone" interim model, at: https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf

[2] https://www.icann.org/en/system/files/files/gdpr-aam1-ipbc-whois-access-accreditation-process-1-3-27mar18-en.pdf

ABOUT THE APWG

The **Anti-Phishing Working Group** (apwg.org) is a not-for-profit research, educational, and industry association, which conducts its activities through a U.S.-incorporated non-profit 501(c)6. APWG's mission is to aid response to cybercrime and cultivate globalized, mutualist responses to it through data exchange, research, and public awareness. The APWG operates cybercrime data exchanges, publishes cybercrime statistics, and presents international cybercrime conferences. It has more than 2,200 members worldwide, including Internet infrastructure and service providers, financial services companies, telecom providers, government CERTs, antivirus firms, and researchers.

APWG.EU (www.apwg.eu) is a chapter of the APWG, and was founded in 2013 as a Spanish non-profit scientific research foundation. APWG.EU's mission is to engage European businesses and organisations in the fight against identity theft and Internet-based crime. As part of this mission, APWG.EU organises and presents at least one cyber-crime convention per year. The foundation is strictly not-for-profit, and is supported by donations, nominal membership fees, and grants.

Among the APWG's activities are:

- Data exchange:
  - Since 2003 APWG has operated its URL Block List (UBL) and successive generations of its progeny, the eCrime Exchange [v.5.2.0], which aggregates machine event reports related to common cybercrime such as phishing from global contributors and distributes those data to browser developers, antivirus vendors, cybercrime responders, forensic analysts and researchers worldwide, delivering hundreds of millions of records per month to its members.
  - The APWG eCrime Exchange (eCX) incorporates the APWG Malicious Domain Suspension (AMDoS) program, now in revision.
  - The APWG's 2018 *Symposium on Policy Impediments to eCrime Data Exchange* will address cybersecurity regulations, laws, treaty conventions, and interpretations that affect the sharing cybercrime event data. This year's program will focus extensively on the provisions of the EU's new General Data Protection Regulation (GDPR).
  - Charter member of the Zero Botnet Alliance, a collaborative effort to track and disseminate threat data related to criminal botnets.
  - The APWG Crypto Currency Working Group helps cryptocurrency exchanges, wallets, investment funds, and consumers protect against phishing and targeted attacks.
  - APWG has authored technical standards for data exchange (RFC5901).
- Research and Education:
  - APWG publishes quarterly and semi-annual reports that provide authoritative metrics about phishing and identity theft.
  - APWG is the organizer of the annual *eCrime Researchers Summit*, the only peer-reviewed conference dedicated to cybercrime studies, the proceedings of which are

published by the IEEE. APWG also organizes and hosts other events each year, including its including its *Symposium on Global Cybersecurity Awareness* in Europe.

- APWG is co-founder and principal architect/organizer of the ***STOP. THINK. CONNECT***. Messaging Convention, the global online safety public-awareness collaborative now deployed by national campaign curators in 19 countries.

- Technical and Public Policy: APWG is an expert advisor and research correspondent to governance bodies, standards organizations, national governments, and treaty organizations. Among them are the Internet Engineering Task Force (IETF), the Council of Europe's Convention on Cybercrime, the United Nations Office on Drugs and Crime, the Organization for Security and Cooperation in Europe and the Organization of American States. The APWG is also on the steering group of the Commonwealth Cybercrime Initiative of the Commonwealth of Nations.

LEGITIMATE ACCESS FOR SECURITY AND STABILITY NEEDS

An accreditation plan for qualified parties to access non-public WHOIS data is consistent with the GDPR's explicit mechanisms to balance the various legitimate public and private interests at stake, including privacy, security, and accountability. Access is justified especially under GDPR recitals 47, 49 and 50,[3] which allow uses "in the public interest" including but not limited to "preventing fraud"; "ensuring network and information security," including the ability to resist "unlawful or malicious actions"; and reporting possible "criminal acts or threats to public security" to authorities. For applicable references from the GDPR, please see Appendix A. Articles 40 to 43 of the GDPR describe the mechanisms and requirements for accreditation programs, including codes of conduct, monitoring of codes of conduct, and certification bodies.

ICANN's Governmental Advisory Committee (GAC) recognizes the above, and recently reiterated that "The current WHOIS system helps achieve many such public policy interests, including enhancing trust in the DNS, ensuring consumer protection, protecting intellectual property, combating cyber-crime, piracy and fraud, to cite but a few of the elements highlighted already in the GAC's 2007 WHOIS Principles."[4]

The APWG's members are engaged in protecting themselves and their customers from an array of threats including phishing, malware, DDoS attacks, and network intrusions. For more than a decade, the APWG has been participating in ICANN and describing how its members rely on WHOIS data for these purposes.[5]

Blocked access to contact data in WHOIS will significantly harm the public interest by hampering legitimate access to critical information which allow parties to enforce laws and contracts, protect consumers, detect and mitigate abuse, and protect critical infrastructure. The Internet is a network of networks that is mainly operated by private parties and self-regulated through contracts and private relationships. Any party can send traffic to another, and the operator of any resource on the Internet has a responsibility to act in an appropriate and accountable fashion. Among other problems, ICANN's proposed access model severely impacts contactability (the ability to reliably identify and/or reach out to domain operators); the ability to identify malefactors; and the ability to correlate data to detect and mitigate abuse and crime.

While law enforcement plays a vital role in investigating and prosecuting crime, law enforcement becomes involved in only a tiny percentage of e-crime and abuse incidents on the Internet. Instead, private entities are the ones on the front lines of Internet security and stability, responsible every

[3] See https://gdpr-info.eu/recitals/ and http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[4] ICANN61 GAC Communique, https://gac.icann.org/advice/communiques/public/20180315_icann61%20gac%20communique_final.pdf

[5] See for example "Advisory on Utilization of Whois Data For Phishing Site Take Down": http://docs.apwg.org/reports/apwg-ipc_Advisory_WhoisDataForPhishingSiteTakeDown200803.pdf and "Trends in Abuse and the Need for Mitigation": https://gacweb.icann.org/download/attachments/44663174/icann58-cross-community-abuse-13mar17.pdf?version=1&modificationDate=1489483612000&api=v2

minute for protecting their networks, services, and users. Indeed, law enforcement relies every day on cooperation with and referrals from private entities who are members of APWG. As Europol's European Cybercrime Centre stated, "Removing the cybersecurity community's access to Whois data will thwart existing cybersecurity mitigation techniques and further empower the ability of cyber attackers to scale their infrastructure with more persistent campaigns. Given the centrality of DNS abuse to an enormous volume of malicious cyber activity, and the current role of cybersecurity companies and independent researchers in defending would-be victims via Whois data, such access remains necessary and is vital to a multi-stakeholder approach to cybersecurity."[6]

Without access to domain name registration data by security operators, investigators, responders, and researchers, the Internet will become a place with much less security, stability, accountability, and ability to regulate itself.

[6] https://www.icann.org/en/system/files/files/gdpr-letter-ec3-europol-icann-proposed-compliance-models26jan18-en.pdf
and https://www.icann.org/en/system/files/files/gdpr-statement-ec3-europol-icannproposed-compliance-models-25jan18-en.pdf

ACCREDITATION PLAN OVERVIEW

At a high level, we assume that the basics are:

1. ICANN approves an accrediting body or bodies.
2. These bodies evaluate applicants and approve (certify) the qualified ones.
3. Approved parties must agree to terms of service that codify compliance with GDPR.
4. Approved parties receive access. Below we describe a short-term access plan that can be implemented quickly by at least some registrars and registry operators. (See "Proposed Operating Model" on pages 10-12.) Longer-term the community will need to come up with a more sophisticated plan that involves industry-wide adoption of the Registration Data Access Protocol (RDAP) protocol and a more sophisticated technical credential system.

ICANN must devise appropriate contractual language that requires the contracted parties to participate in the accreditation program, with participation requirements that will be effective and can be enforced by ICANN's Compliance Department. **In the short term this could be done via a Temporary Policy**[7]. This would allow lawful access to the data and would allow up to one year for ICANN Org to create modifications to the RAA and registry contracts, and to deploy the RDAP protocol, which would then allow for a more sophisticated, longer-term technical implementation.

This plan will help fulfill the ICANN GAC's Consensus Advice[8] to:

- "Ensure continued access to the WHOIS, including non-public data, for users with a legitimate purpose, until the time when the interim WHOIS model is fully operational, on a mandatory basis for all contracted parties" and
- "Ensure that limitations in terms of query volume envisaged under an accreditation program balance realistic investigatory cross-referencing needs" and
- "Consider the use of Temporary Policies and/or Special Amendments to ICANN's standard Registry and Registrar contracts to mandate implementation of an interim model and a temporary access mechanism".

[7] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary

[8] https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee?preview=/27132037/53674097/20180315_ICANN61%20GAC%20Communique_Final.pdf

COMMENTS ON THE "1.3 MODEL" ("CANNOLI") BY THE IPC and BC

Below we comment on the "Model 1.3" or "Cannoli Model" proposed by ICANN's Intellectual Property Constituency and Business Constituency.[9] That plan (described on pages 4-14 of the 1.3 draft) lays out a rational framework. APWG supports "Model 1.3"with the modifications below and looks forward to helping make refinements.

Section 1: Cybersecurity & OpSec Investigators

The list of examples of services covered should include "financial services". The list of examples of entities in this category should include HSBC, JPCERT/CC, and REN-ISAC.

Section 2: Intellectual Property

We note that cybersecurity and operational security actors in Section 1 may occasionally use intellectual property issues as a legitimate reason for accessing non-public WHOIS data. As examples, phishing is criminal theft that also involves consumer confusion and misappropriation of trademarks, and some security actors address consumer fraud and product counterfeiting, which involve both fraud and intellectual property violations.

Validation and Review of Access Purposes

Further below we comment regarding remedies for inappropriate use.

Legitimate and Lawful Purposes

We note that cybersecurity and operational security actors use domain registration data for purposes in multiple categories here, including Legal Actions, Security/DNS Abuse Mitigation, Forensic Analyses, Contractual Enforcement, and Public Health and Safety.

Process for Vetting and Accreditation

Regarding "Cybersecurity & OpSec Investigators: Verifiable credentials and letters of authority": we note that the term "credentials" will need appropriate definition, and examination by each accrediting body. In general the goal is for applicants to prove their identity, qualifications and achievements, and provide evidence that they are suitably skilled and competent to observe the data protection requirements attendant accessing non-public WHOIS data. In the security sphere, some entities will be able to present "official" certifications (for example banks possess government charters). Other security practitioners operate in spheres that are not similarly regulated or licensed.

Proposed Operating Model

We propose an alternate plan that we believe may be easier to implement for the shorter term.

[9] https://www.icann.org/en/system/files/files/gdpr-aam1-ipbc-whois-access-accreditation-process-1-3-27mar18-en.pdf

The "Cannoli Model" proposes "Upon accreditation, users are given credentials to access Whois data. Users are able to present their credentials to a Whois database operator who validates credentials with a federated, centralized access authority and then provides access to Whois data." Such a credentialing system cannot be built quickly. Instead, our plan avoids those problems.

Our proposal for the short term is:

1. **Approved parties designate their rationale for access under GDPR, i.e. their legitimate reasons for accessing the data and the use(s) they will put it to.**
2. **Approved parties designate the IP addresses from which they wish to query WHOIS servers.**
3. **The accrediting bodies provide those IP addresses to ICANN, which collects them into a single list.**
4. **All WHOIS server operators (registries and registrars) will be required to pick up that list from ICANN on a daily basis. They must white-list WHOIS access from the approved IP addresses, and provide full WHOIS data ("thick" data, containing contact data) for queries coming from those IP addresses.**

Port 43 access managed by IP range is appropriately secure -- it ensures that only approved parties can gain access to the non-public data. The registries and registrars can log queries by IP and thus by accredited user.

GoDaddy already offers exactly this tiered access service on its port 43 servers. Anonymous users who query GoDaddy's WHOIS server cannot view contact data. But GoDaddy recognizes the IP addresses of authorized users, and provides them with full WHOIS responses that contain contact data.[10]

Some registrars already log what WHOIS queries are made for what specific domain names, by IP addresses.[11] All major industry players already use IP addresses to impose rate-limiting on their port 43 servers, and use white-listing to give authorized users higher query limits. Offering tiered WHOIS access to authorized IP addresses is a modification of this practice. We believe that many parties could implement our proposed solution, as GoDaddy has, at least as easily as any other solution. The major industry players all have the technical wherewithal to make the changes on an expedited schedule, and together they manage the majority of gTLD domain names.

The "Cannoli Model" also requests a *centralized access point*. Specifically it proposes access leveraging the existing ICANN web-based centralized Whois system[12]. Web-based access is designed for human users and single lookups, and is not suitable for automated access. APWG emphasizes that port 43 access is vital because it allows users to make automated, *machine-based* queries. And in the short-term, creating a central access point at ICANN (or anywhere else) would be a project involving 1) credential management (distributing usernames and passwords to users), and 2) a query logging system operated at ICANN, *and* 3) requires the server operators to provide tiered access to ICANN's system (i.e.

[10] https://www.godaddy.com/help/masking-contact-information-shared-via-whois-automated-access-points-27421

[11] For example see https://domainnamewire.com/2018/01/11/tracking-whois-searches-decide-domain-renewals/ and https://domainnamewire.com/2018/01/16/epik-takes-whois-search-counts-another-level/

[12] https://whois.icann.org/en/lookUP?name=

provide tiered access by IP). These all can't be implemented quickly. Our plan avoids tasks #1 and #2 entirely. If web-based access is needed by some users, perhaps an approved entity can build access for other approved users, providing usernames/passwords and logging queries as needed.

Over the longer term, we agree that a more sophisticated mechanism should be developed. Registries and registrars will need to adopt RDAP, which offers additional authentication features and more granular control of output. RDAP deployment will not happen for some time--at least six months from when ICANN Org and the contracted parties agree on a deadline. Between now than then, parties could work out the implementation and rollout details.

We must avoid a situation in which every accredited party must go to every single registrar and registry operator and seek access or credentials from them individually. That situation is a nightmare for all involved and is highly impractical. ICANN faced a similar situation when the new gTLDs launched and parties would start seeking zone file access for the thousand-plus new gTLDs. The ICANN community solved that problem by establishing the Centralized Zone File Access System (CZDS), which offers a centralized place for parties to manage their subscriptions.

Logging

- Registries and registrars will be able to log what parties are querying which domain names. ICANN must ensure that this log data remains confidential under all cases. Revealing that data to registrars or other parties could compromise investigations, especially by law enforcement.
- Regarding "Logs will include accredited entity, purpose, query, and data": granular sophistication will be possible under a longer-term, RDAP-based system.

Central Access Authority

The "Cannoli Model" states that "Application and renewal fees should be sufficient to cover onboarding and support fees for the authorization and access system." ***We disagree***, for the following reasons:

1. This would be tantamount to charging for WHOIS access. It should never be charged for. ICANN's historical approach -- reflected in its registry and registrar contracts and its new gTLD application program -- has always been that:
    a. WHOIS is a public resource.
    b. WHOIS is provided for a wide variety of legitimate uses and is necessary for the stability, security, and trustworthiness of the namespace and the Internet in general.
    c. WHOIS is a core service provided by registries and registrars. It is not a value-added or revenue-generating service.
2. Charging for WHOIS would shift costs from malefactors to the defenders who keep the Internet safe.
3. The suggestion is unfair to the certifying organizations and the certified users users, who will likely have no control over the costs incurred by the party running the authorization and access systems.

Instead, the authorization and access system is an appropriate use of ICANN funds. This is an essential infrastructure support service of the type that ICANN exists to maintain, and it is no different from having ICANN fund and operate the CZDS. Also, GDPR imposes certain new costs on registrars and

registry operators. This is a simple consequence of the legislation, and is part of doing business in the European Union and servicing customers in EU member states. Passing those costs on the Internet defenders is not appropriate. The appropriate solution is to subsidize the costs via registry and registrar fees.

The "Cannoli Model" states that "Login and authorization for access by accredited entities to Whois database operators at registries and registrars will be provided by a third-party or parties." Or, it might be provided by ICANN. The mechanics of a federated, centralized access authority need to be worked out.

Penalties

We believe that de-accreditation and referral to EU privacy authorities are the effective and practical remedies. These are the steps required by the GDPR's Article 41.[13]

The "Cannoli Model" suggests "financial penalties" imposed by the accrediting bodies. This should be stricken. Under the law, the EU authorities have the primary responsibility for seeking financial penalties for non-compliance with GDPR. It may not be possible for accrediting bodies to impose financial penalties under contract law, which in many countries permit actual damages for breach of contract (established by a court or arbitration) but not punishment (punitive damages). (This is a reason why ICANN's registry and registrar contracts do not contain escalating financial penalties for non-compliance.) Finally, private parties have direct legal recourse against accredited users who violate their rights.

Data Access

We agree that accredited access should not be rate-limited except to prevent system overload. In its latest Consensus Advice, the GAC advised the ICANN Board to instruct the ICANN Organization to "Ensure that limitations in terms of query volume envisaged under an accreditation program balance realistic investigatory cross-referencing needs".[14] This means that registrars and registry operators must not impose rate-limiting on accredited users that would prohibit them from making enough WHOIS queries to do their work. Some security operators need to perform significant numbers of queries so that they can find and monitor abuse across large numbers of domains and find bad actors registering across TLDs and registrars. **This piece of advice needs to be incorporated into any Temporary Policy in the short term, and into contracts longer-term.**

[13] http://www.privacy-regulation.eu/en/article-41-monitoring-of-approved-codes-of-conduct-GDPR.htm

[14] https://gac.icann.org/advice/communiques/public/20180315_icann61%20gac%20communique_final.pdf

OTHER NOTES REGARDING TECHNICAL IMPLEMENTATION

In a recent letter to ICANN[15], the Contracted Parties raised several complications to the introduction of any access system. Our evaluation of those objections are as follows:

- "Creating a centralized credentialing system will take significant time, as it will require input from across the ICANN community." Our short-term plan does not require a true centralized credentialing program.
- "The timeline for that effort will be measured in quarters (or possibly years), rather than months, due to the complexities inherent in disclosing data across jurisdictions and other factors." ICANN's Interim Model states that all registrars will continue to transfer contact data to registries and escrow providers, assumes that registration data will cross borders, and states that an accreditation process is a legally viable option. As such it does not recognize cross-border transfer as a concern that should delay access.
- The Contracted Parties plan "assumes that individual contracted parties will need to handle credentialing in the meantime in order to continue providing access to non-public WHOIS data", and that each registry and registrar "independently develops internal policies for what parties can get access, what data elements those parties can access once credentialed (recognizing that unlimited access to all WHOIS records for every credentialed parties is not likely to be compliant under GDPR), procedures for processing requests, etc." We question these assumptions. Allowing each operator to come up with its own policies and procedures will be a disaster. It will result in loss of access to many registries and registrars even for law enforcement, will make it very difficult for other users who have legitimate right to access the data, and will not be an enforceable situation for the ICANN Compliance Department . It is the kind of non-scalable situation that ICANN decided was unacceptable for zone file access (see above). Instead, it is the responsibility of ICANN to put a predictable and enforceable model in place.
- The Contracted Parties only offer one solution for automated access — RDAP. Our short-term plan continues the use of port 43 WHOIS until RDAP is deployed.

[15] https://www.icann.org/en/system/files/files/gdpr-comments-contracted-parties-cph-timeline-icann-proposed-compliance-models-26mar18-en.pdf

APWG PARTICIPATION IN CERTIFICATION PLAN

Per Articles 40 to 43 of GDPR, ICANN evidently must present an accreditation plan to an EU Supervisory Authority. The "Article 29 Working Party Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679"[16] is the relevant guide to accreditation. Those Guidelines state there must be an established *certification body* (or bodies), a "third-party conformity assessment body operating a certification mechanism." That certification body will undertake *certifications* of parties seeking access to non-public WHOIS data. Certifications are "the assessment and impartial, third party attestation that the fulfilment of certification criteria has been demonstrated" and that a party is conformant and can access the data. A *scheme owner* is "an identifiable organisation which has set up certification criteria and the requirements against which conformity is to be assessed. The accreditation is of the organisation that carries out assessments (Article 43.4) against the certification scheme requirements and issues the certificates (i.e. the certification body, also known as conformity assessment body). The organisation carrying out the assessments could be the same organisation that has developed and owns the scheme, but there could be arrangements where one organisation owns the scheme, and another (or more than one other) performs the assessments."

The GAC does not appear interested in having an operational role. It appears to us that ICANN may be the "scheme owner." ICANN needs to either act as a certification body or arrange for a certification body or bodies to perform assessments.

APWG is willing to help craft specific accreditation procedures, including what kinds of documentation and *bona fides* should be required of applicants, specifically security actors and researchers.

APWG is also willing to consider helping to assess APWG members who wish to apply, if it is determined that such an arrangement is practical and conformant with the law. If APWG does so, the applicants who we would examine would first need to be APWG members. Those applicants would then be required to pass additional screening and requirements as required by the certification body. APWG envisions itself as one, non-exclusive body doing this kind of work. We have membership and expertise in the security and anti-abuse realm, and wish to focus our work to that area of expertise. APWG hopes and assumes that other bodies will step forward to serve other user communities who need vetting.

APWG has experience in this area. The APWG Malicious Domain Suspension (AMDoS) system[17] enables specially accredited Interveners to submit suspected malicious domain names for investigation and suspension by participating registry operators and registrars. APWG vets malicious domain reporters (Accredited Interveners), and the AMDoS system systematizes suspension requests through a formal process that ensures the credibility of malicious domain reporters and integrity of their suspension requests and speeds them on their way to the Registrars of record.

[16] http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877
[17] https://www.antiphishing.org/apwg-news-center/amdos/

Appendix A: Justifications for Processing under Recitals in GDPR

Emphases in **bold** have been added.

Recital 4 Data protection in balance with other fundamental rights

1The processing of personal data should be designed to serve mankind. **2The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality**....

Recital 47 Overriding legitimate interest

1 The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

2 Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

3 At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

4 The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

5 Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.

6 The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.

7 The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Recital 49 Network and information security as overriding legitimate interest

1 The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or 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, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."

Recital 50 Further processing of personal data

1 The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.

2 In such a case, no legal basis separate from that which allowed the collection of the personal data is required.

3 If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.

4 Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing.

6 In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data

have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

1 Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes.

2 In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured.

3 Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller.

4 However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

Recital 156 Processing for archiving, scientific or historical research or statistical purposes

1 The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

2 Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation.

3 The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfill those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data).

4 Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5 Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information

requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6 The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles.

7 The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

Recital 157 Information from registries and scientific research

1 By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression.

2 On the basis of registries, research results can be enhanced, as they draw on a larger population.

3 Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions.

4 Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services.

5 In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

19 April 2018

Dear ICANN,

On behalf of the Board of Directors of the Forum of Incident Response and Security Teams (FIRST), we wanted to take a brief moment to follow up on our message dated March 15th, 2018.

Over the last few weeks, FIRST has been collecting experiences of our members in their **use of the WHOIS directory and services**. Our members see WHOIS as a valuable resource for abuse reporting, incident response and security investigations. We have shared some of these thoughts on our web site at https://www.first.org/blog/.

Some of the clearest and most common examples of its use in security include:

- Frequent use of WHOIS data to determine where to send a takedown request of malicious code or phishing sites, or to contact the owner of a site to notify them that the site has been compromised;
- Determining whether or not a site is registered by an individual or organization that has previously registered a domain name which was used for malicious purposes, or that is the registered name holder of domain(s) currently being used maliciously.

Access to WHOIS for the security community is essential in the fight against cybercrime. A prolonged interruption will only profit criminals, and negatively affect privacy of internet users.

As an association of organizations in the security response community, **FIRST encourages the ICANN Board to instruct ICANN org to move forward with a sense of urgency to implement an accreditation plan for access to WHOIS**. We support the previous recommendations by APWG and M3AAWG to establish a community group, including the anti-abuse and incident-response communities, to facilitate the creation of an accreditation model for qualified applicants from the security community. FIRST welcomes any opportunity to participate in such an expert task force to draft those requirements, and to contribute our perspective as an association of over 414 security teams in 85 countries.

We believe an **enforceable interim model**, while the accreditation requirements are being developed, is critical to ensure continued access to WHOIS data beyond May 25th, 2018. We reviewed the comments by the WP29 regarding the lack of security controls on IP-based access to WHOIS data. We agree there are limitations to the ability of IP-based authentication to provide significant levels of security.

However, it does propose an already supported, well understood and maintainable step-based approach over today's lack of authentication. While a more sophisticated mechanism will need to be designed and developed to provide long-term accredited access, we support the proposal to enforce use of an intermediate IP whitelist for access to WHOIS data for anti-abuse, threat intelligence, and incident response while the accreditation plan is being implemented. Temporary disruption of continuous access for security purposes such as incident response, abuse reporting, threat intelligence and anti-abuse is otherwise likely to impair the technical and organisational security measures that are being relied on currently to ensure a reasonable level of security.

Therefore, we specifically recommend that the ICANN org create a special task force of security experts to sketch out how the IP-based access could be implemented in a manner that mitigates the WP29 concerns while still protecting the security of the unique identifiers during any interim period to avoid a blackout in May. Any such temporary policy will require careful consideration of rate limiting alongside the white listing.