SAC061
SSAC Comment on ICANN's Initial Report from the Expert Working Group on gTLD Directory Services

A Report from the ICANN
Security and Stability Advisory Committee (SSAC)
9 September 2013

Preface

This is a Comment to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning the Initial Report from the Expert Working Group on Next Generation Directory Services. The SSAC advises the ICANN community and Board on matters relating to the security, stability and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Comment, references to SSAC members' biographies and statements of interest, and SSAC members' objections to the findings or recommendations in this Comment are at the end of this Comment.

Table of Contents

Executive Summary

The Initial Report from the Expert Working Group (EWG) on Next Generation Directory Services (hereinafter referred to as the "EWG Initial Report") proposes paradigm shifts from norms that have been in place for many years. These shifts include proposed changes to how domain registration data is stored and accessed, and proposals for broad limitations on who can access what data and for what purposes.

In this comment, the SSAC describes four substantive issues with the EWG Initial Report: 1) Purpose of Registration Data, 2) Availability Risks, 3) Authentication and Access Control and 4) Data Accuracy.

The SSAC proposes the following four recommendations for the EWG to consider:

Recommendation 1: SSAC reiterates its recommendation from SAC055: The ICANN Board should explicitly defer any other activity (within ICANN's remit) directed at finding a 'solution' to 'the WHOIS problem' until the registration data policy has been developed and accepted in the community. The EWG should clearly state its proposal for the purpose of registration data, and focus on policy issues over specific implementations.

Specifically, SSAC does not believe the EWG has answered the question of the purpose of registration data. A clear statement of the purpose is essential before a thorough and complete risk analysis can be completed of the proposed next generation directory services.

Recommendation 2: The ICANN Board should ensure that a formal security risk assessment of the registration data policy be conducted as an input into the Policy Development Process.

A separate security risk assessment should also be conducted regarding the implementation of the policy.

Recommendation 3: SSAC recommends that the EWG state more clearly its positions on the following questions of data availability:

A. Why is a change to public access justified? This explanation should describe the potential impact upon ordinary Internet users and casual or occasional users of the directory service.

B. Does the EWG believe that access to data currently accessible in generic Top Level Domain (gTLD) WHOIS output should become restricted? If so, what fields and to what extent exactly? Under the EWG proposal, queries from non-authenticated requestors would return only "public data available to anyone, for

any purpose".[1] At this time it is unspecified what the set of "public data available to anyone" is, and therefore it is unclear if the infrequent or non-professional users will lose access to data they rely upon, when they need it. It appears that Annex C may recommend that non-authenticated users be denied access to several data elements that they can access today via WHOIS. Annex C also neglects to mention Administrative, Technical, and Billing contacts. Will access to a currently public source of data be degraded and made less useful for a large number of users so that a smaller number of users can receive enhanced access, and if so why is such a shift justified?

C. Should all gTLD registries be required to provision their contact data into the Aggregated Registration Data Service (ARDS)? There may be jurisdictions that prohibit by law the export of personally identifiable information outside the jurisdiction. If so, the ARDS may not be a viable way to deliver data accuracy and compliance across all gTLDs.

D. Does the EWG propose more types of sensitive registration data be provisioned into ARDS than are found in current gTLD WHOIS output? This question was left unanswered in Annex C. Proposals to do so should be justified.

    a. For example, the EWG listed the Internet Protocol (IP) address of the registrant as a type of registration data.[2] Does the EWG propose that this data be provisioned by registrars to the registries, and then from the registries into the ARDS and made available to those parties with a need to perform the stated purpose of "Abuse Mitigation"? In such cases, the EWG needs to demonstrate a justification that goes beyond saying that the provisioning of such data would "serve the purpose" of certain data consumers. Instead, the question is whether giving additional parties access to such data is a good idea, and how it might be justified.

    b. The EWG also listed "EPP Transfer Key" as a type of registration data. We assume this is the EPP auth_info code for a domain. The provisioning of EPP auth_info codes into a meta-registry poses a major security risk and should never be allowed.

[1] EWG Draft report, page 35.

[2] EWG Draft Report, page 45. This means the IP address from which the domain registration was made, *not* the A record(s) of the domain name.

[2] EWG Draft Report, page 45. This means the IP address from which the domain registration was made, *not* the A record(s) of the domain name.

Recommendation 4: The SSAC suggests that the EWG address this recommendation from SAC058: "SSAC Report on Domain Name Registration Data Validation"[3]:

> *As the ICANN community discusses validating contact information, the SSAC recommends that the following meta-questions regarding the costs and benefits of registration data validation should be answered:*
>
> - *What data elements need to be added or validated to comply with requirements or expectations of different stakeholders?*
> - *Is additional registration processing overhead and delay an acceptable cost for improving accuracy and quality of registration data?*
> - *Is higher cost an acceptable outcome for improving accuracy and quality?*
> - *Would accuracy improve if the registration process were to provide natural persons with privacy protection upon completion of multi-factored validation?*

1. Introduction

This document comments on several areas of the Initial Report from the Expert Working Group (EWG) on Next Generation Directory Services[4] (hereinafter referred as the "EWG Initial Report"). The SSAC thanks the EWG for its work on this difficult subject. The EWG Initial Report proposes paradigm shifts from norms that have been in place for many years. These shifts include proposed changes to how domain registration data is stored and accessed, and proposals for broad limitations on who can access what data and for what purposes. The SSAC is of the opinion that if implemented, the EWG Initial Report's contents may have profound implications for registrant data security, registry and registrar security and stability, and for the safety of ordinary Internet users who rely on that data to understand the trustworthiness of services and products offered through domain names.

Security and stability requires balancing risks, benefits, and costs. The SSAC does not believe the EWG Initial Report provides adequate explanations of the proposed policies and their perceived benefits and risks, or how they were balanced. It proposes some specific solutions, but neither lists other potential options nor justifications for the proposed solutions. The creation of the Aggregated Registration Data Service (ARDS) would also likely introduce significant new security and stability risks, and it is unclear if those new problems will offset the benefits the service would provide.

---

[3] See SSAC Report on Domain Name Registration Data Validation (27 March 2013) at http://www.icann.org/en/groups/ssac/documents/sac-058-en.pdf.

[4] Internet Corporation for Assigned Names and Numbers (ICANN) 2013."Initial Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service at: http://www.icann.org/en/groups/other/gtld-directory-services/initial-report-24jun13-en.pdf.

Given the complexity of the issues and the evolving nature of the EWG Initial Report, the following document does not attempt to address all of the security and stability issues involved. The SSAC will track the evolving discussion closely, and plans on providing additional input as the process proceeds. Since the proposals may have far-reaching consequences to the Internet community-at-large, registrars, and registries SSAC expects that those policies and implementation ideas that the ICANN community finds of potential merit will be subject to the formal Policy Development Process.

2. Findings

The SSAC describes four substantive issues with the EWG Initial Report in the following sections: 1) Purpose of Registration Data, 2) Availability Risks, 3) Authentication and Access Control and 4) Data Accuracy. While these four issues are not exhaustive, they do identify principal concerns the SSAC has with respect to the proposals found in the EWG Initial Report.

2.1 Purpose of Registration Data

In September 2012, the SSAC published advisory SAC055[5]: "WHOIS: Blind Men and an Elephant," which commented on the recommendations of the WHOIS Review Team. It made three recommendations to the ICANN Board of Directors:

1. *The Board should pass a resolution clearly stating the criticality of the development of a registration data policy defining the purpose of domain name registration data, and*
2. *The Board should direct the CEO to create a registration data policy committee that includes the highest levels of executive engagement to develop a registration data policy which defines the purpose of domain name registration data, as described elsewhere in this document* [SAC055]; *and*
3. *The Board should explicitly defer any other activity (within ICANN's remit) directed at finding a "solution" to "the WHOIS problem" until the registration data policy identified in (1) and (2) has been developed and accepted by the community.*

The Board acted on the first two recommendations, creating the EWG. Regarding the third recommendation, the Board chose a different course and tasked the EWG with both defining the purpose of collecting and maintaining gTLD registration data, and providing a proposed solution for managing gTLD directory services.[6]

[5] See ICANN Security and Stability Advisory Committee (SSAC) 2012. "WHOIS: Blind Men and an Elephant," (SAC055) at: http://www.icann.org/en/groups/ssac/documents/sac-055-en.pdf.
[6] See http://www.icann.org/en/news/announcements/announcement-2-14dec12-en.htm.

The SSAC does not believe the questions of policy and of defining "the purpose of registration data" have been answered within the EWG Initial Report. In SAC054: "SSAC Report on the Domain Name Registration Data Model", the SSAC suggested that the purpose of registration data is to serve the needs of the lifecycle of a domain name.[7]

The EWG appears to have taken a different approach, focusing the purpose on the various consumers of the data. If the EWG believes that the purpose of the data is to serve the various use cases identified in the report, the SSAC believes the EWG needs to further explain that interpretation of the purpose of registration data in its report. Questions that would need to be considered include the following.

- What constitutes a valid use of registration data and who makes that decision?
- How is the list of valid uses of registration data to be managed?
- Will registries, registrars and others, as needed, be subject to changing requirements based on the petitions of future user communities with valid uses?

Answering at least these questions clearly and directly will help ensure understanding of the "why you collect it" question asked in SAC055, will help specify the data that needs to be collected, and will assist in defining the process needed to collect it as well as how the data should be stored and accessed. After a collection process and methodology is determined, a process regarding why various communities should have access to what data can be undertaken. More succinctly, the SSAC believes a model for access to data, including who should access the data, should not be proposed until there is an understanding of what data has been collected and why it has been collected.

The EWG, in parallel to proposing a new model for the purpose of registration data, discussed several "system designs" for access to the data and proposed one model, calling for a centralized registration data repository.[8] That approach poses a quandary: policies are expressions of goals and should articulate the problems the community designed them to solve. Until proposed registration data policies and their justifications are stated clearly, it is not possible to comment definitively on their security and stability consequences. And until the community accepts the policies, it is difficult to discuss whether proposed delivery options will satisfy the goals in a suitably secure and stable manner.

Improving and ensuring security and stability require balancing risks, benefits, and costs. While it is understood that the EWG Initial Report is a first attempt by the EWG to address these issues, the SSAC does not believe adequate explanations of the perceived benefits, risks, or costs, or how they were balanced has been provided. The EWG Initial Report describes some proposed solutions but does not always discuss why those

[7] See SSAC Report on the Domain Name Registration Data Model (11 June 2012) at: http://www.icann.org/en/groups/ssac/documents/sac-054-en.pdf.
[8] See EWG Draft Report, page 4.

solutions are justified. Instead, the report focuses on a specific outcome: a specific system with many features. The EWG Initial Report did not state what alternatives it considered and rejected and did not indicate the EWG's methodology for developing its recommendations. Some of the items in the EWG's list of "Desired Features and Design Principles" (pages 20-27) may be seen within the community as new policies, and some are feature requests and implementation choices that may be only some of the possible ways to execute on the policies. If the ICANN community does not accept some of the proposed policies, the features and implementation choices will necessarily change.

The SSAC believes a centralized meta-registry (e.g., the ARDS) is not the only solution to problems stated by the WHOIS Review Team, and it is unclear whether that specific solution will create net improvements when weighed against the risks.

2.2 Data Availability Risks

The ARDS is proposed as the sole source of generic Top Level Domain (gTLD) registration data to the global Internet community. Reliance on a single system or provider carries a significant risk. There are ways to manage these risks, such as measures to prevent distributed denial-of-service (DDoS) attacks and directed attacks to gain unauthorized access to the information, but such measures have costs associated with them. Those costs for an ARDS would be high given the unforgiving 100 percent uptime requirement and large load (at least ten billion queries per month and possibly much more[9]). It is self-evident that the ARDS would be an attractive target for miscreants, and therefore a thorough and complete assessment of those risks is essential.

The EWG proposed that ICANN should create a system that issues "globally unique" identifiers to all gTLD registrants, and that "no domain names should be registered with an identical name/organization without supplying this auth code."[10] This implies that the ARDS will be the authoritative repository of those identifiers, and implies that all registries must query the ARDS before creating a domain name.[11] This would make all gTLD registries operationally dependent upon the ARDS system. That would introduce a new, very serious registration stability risk, and a potential operational performance penalty (latency) that cannot be controlled by either the registry or the registrar.

The EWG Initial Report stated "The ARDS can also provide access to live registration data that is obtained in real-time from gTLD registries." This means that the ARDS will need to maintain connections to all gTLD registries, so that data can be pulled directly from the registries on demand. This will require the ARDS operator to maintain secure and appropriately permissioned connections to more than 1,000 registries, and to monitor and prevent misuse of that access.

[9] The number of WHOIS queries for .COM alone was more than 8.3 billion in April 2013, according to the ICANN registry operator report: http://www.icann.org/en/resources/registries/reports/com/com-apr13-en.pdf

[10] See EWG Draft Report page 24, 4.9.3 and 4.9.4

[11] And also transferring a domain name to a new registrant.

In which legal jurisdiction would the ARDS reside? This could cause issues from a multi-stakeholder trust perspective. It raises issues about variances in geographic privacy laws, data retention laws, and lawful rights for accessing data residing within the ARDS.

Some Internet users -- not just professional investigators and law enforcement -- use domain registration data to determine who has registered a domain name, and to decide whether the services offered there are trustworthy. Consumer protection agencies recommend that consumers use WHOIS to protect their interests. Both empirical and anecdotal evidence show that this advice is followed. For example, Federal Trade Commission (FTC) staff recently searched the FTC's database of consumer complaints and found a significant number of references to the term "WHOIS." These results indicate that when consumers encounter problems online, the WHOIS databases are a valuable initial tool they use to identify with whom they are dealing.[12] Consumers often protect themselves by looking at who is offering goods or services via a domain name, and they report abuse and scams on forums and to consumer protection bodies. The current WHOIS system has problems, but for these users the current anonymous access to registration data clearly has utility. The SSAC does not believe the EWG has clearly stated why a change to public access is recommended.

The SSAC does not believe the risks of the ARDS system have been sufficiently investigated. A thorough investigation of the risks, and the cost of mitigating those risks, is necessary if the community finds the concept of the ARDS of further interest.

2.3 Authentication and Access Control

The EWG proposes that all users who wish to obtain gTLD registration data from the system must apply for access credentials, and will be permitted a level of access that depends on their needs, for permissible purposes only. The creation of such a centralized, global authentication and monitoring regime is a significant undertaking and its implementation is fraught with security and stability challenges including but not limited to:

1. *Managing the number of applicants and the credentials of each applicant.*
   It is not a best security practice for users within an organization to share the same access credentials, so each individual user should be issued access credentials tied to their parent organization and its role(s). The maintenance of access will be especially complicated with users who will have enhanced access because of the expected increase in authentication requirements.

[12] See the following resources: www.icann.org/en/news/presentations/hiramatsu-mar-26jun06-en.pdf; http://www.ftc.gov/os/2006/07/P035302PublicAccesstoWHOISDatabasesTestimonyHouse.pdf, Section IV; Financial Services Information Sharing and Analysis Center (FS-ISAC)/Internet Crime Complaint Center (IC3)/FBI/U.S. Secret Service at: http://www.ic3.gov/media/2010/workathome.pdf; Better Business Bureau at: http://www.bbb.org/us/article/tips-to-avoid-online-escrow-fraud-553 and at: http://wisconsin.bbb.org/useful-links/; European Consumer Centres France at: http://www.europeconsommateurs.eu/fileadmin/user_upload/eu-consommateurs/PDFs/publications/brochures/Conseils_pour_acheter_en_ligne_sur_un_site_etranger.pdf; and ICANN at: http://www.icann.org/en/help/disputeresolution#services

2. *Making appropriate judgments about applicants in the face of a global constituency.*

   Real challenges will exist in specifying how various entities will be awarded different levels of access rights, and managing that process. Making access decisions when applicants reside in a broad range of geographical, jurisdictional, and political realms is a task with quite a few failure modes. For example, what is considered a law enforcement body, how would those be validated, and should some of those bodies enjoy access levels that are higher than others? In the United States alone, thousands of criminal law enforcement organizations contribute to the annual Federal Bureau of Investigation crime statistics report,[13] and civil law enforcement entities that need domain registration data (such as the U.S. Federal Trade Commission and the U.S. Securities and Exchange Commission) are not part of those numbers.

   The ARDS operator, via the ICANN policies and contract that govern it, may be incentivized to avoid risk and grant access in a conservative way, in which case users will not get the data they reasonably need and deserve, and security and safety could suffer overall. Or access could be granted too liberally, in which case the control regime will be ineffective and may even cause harm by providing bad actors access to controlled information.

3. *Ensuring the security of access credentials, meta-data, and connected systems.*

   A centralized authentication regime would contain information that is even more sensitive than the domain registration data.[14] A breach of its security could be catastrophic. Possible consequences include the compromising of law enforcement investigations, looting of the registration data, the revelation of how business competitors are researching each other, and the compromise of individuals' personal privacy.

   The ARDS and this centralized authentication regime share the requirement to mitigate the risks associated with any centralized system. However, the data in ARDS is vulnerable to a failure of the security of the centralized authentication regime. A risk assessment of this relationship and appropriate mitigation strategies are essential to the security and stability of the ARDS.

4. *Managing the roles of users.*

   In the section "Identifying the users of the RDS" (pp. 11-14), the EWG lists different "users." These might be more properly defined as "roles." An individual or entity may have different reasons for accessing registration data over time, and therefore has many roles over time. For example, one day a company may register a domain name, may later wish to register another domain name and

[13] See http://www.fbi.gov/stats-services/crimestats

[14] The ARDS permissions system would contain records of the identities, usernames, and access credentials of all approved users; the roles and access level of each user; and logs of what data each authorized user accessed, when, and for what purpose. These are necessary for the access control, auditing, and compliance functions that the EWG describes.

confirm the domain's current registrant, and later may need to perform research on an attack affecting its network perpetrated via another domain. Current WHOIS access allows this user to act in all these roles. Users may not anticipate all of their potential roles, and it may be difficult or impossible for them to demonstrate their roles to a central authority and thereby gain access to the data they need. A centralized, permissions-based system may prevent users from accessing data they reasonably need for their roles.

2.4 Data Accuracy

The EWG states that a central purpose of the ARDS is to improve the accuracy of domain contact information. Accuracy has at least three aspects: a) ensuring accuracy at creation time; b) checking its accuracy through its validity period; and c) having compliance mechanisms to address inaccuracy at these two stages. Under the EWG proposal, the operator of the ARDS would be responsible for performing verification checks on contact data, and would take on the compliance role for non-accurate data. The ARDS is also designed as a mechanism for reducing public access to data.

Accurate and available data is important for a variety of security and stability purposes. Among others, it allows interested parties to reach the entities responsible for the domain in order to report problems; it allows Internet users to investigate the trustworthiness of services offered via a domain;[15] it is vital to law enforcement and anti-abuse efforts;[16] and it is central to the process of issuing security certificates.[17] Millions of Internet users rely on domain registration data for their online safety and security. Some users rely on it by looking up the data themselves. And many more rely on the protections provided by service providers who look up the data, including antivirus vendors, block list providers, certificate authorities, search engines, and browser manufacturers. The historical norm has been that registration data (including contact data) has been publicly available, via anonymous means, free of charge, from both port 43 and web-based interfaces. An exception is when the laws of the registry's home jurisdiction prohibit the publication of registrant contact details, such as the details of individual, noncommercial registrants. A number of the new gTLD registries may be located in such jurisdictions.

[15]The WHOIS Review Team commissioned a consumer study, a finding of which was: "If concerned that a website is fraudulent, 68% of International and 65% of National users would "Find Website Contact Information" first and "Search for User Reviews" as a second step users (59% of International and 61% of National)". WHOIS Team Final Report, page 75.

[16]See Anti-Phishing Working Group: "Advisory on Utilization of WHOIS Data For Phishing Site Take Down," http://docs.apwg.org/reports/apwg-ipc_Advisory_WHOISDataForPhishingSiteTakeDown200803.pdf.

[17] The CA/Browser Forum's "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" requires certificate authorities to communicate with domain contacts listed in WHOIS before issuing certificates, and contains guidelines about obtaining authorizations from domain name Registrant, Administrative, and Technical contacts. See https://www.cabforum.org/Baseline_Requirements_V1_1_5.pdf.

Of the data fields currently displayed in existing gTLD WHOIS output, only contact data has a level of sensitivity. All other currently available registration data is either not sensitive (such as a domain's creation date or sponsoring registrar), or is available via other means (for example, name servers and IP addresses can be obtained by a query to the Domain Name System (DNS) or from zone files, when the data is published, i.e., creating a domain name does not require that it resolve). Therefore there does not seem to be any justification for limiting access to those data fields.

The EWG did not state whether contact data across the board generally deserves more protection than it receives now, and if so why.[18] More protection can address issues of accuracy where any unauthorized modification to data can render that data inaccurate. A policy statement about these questions, validated in the community, would then enable a conversation about how to deliver on that policy in a secure fashion. More details are needed from the EWG regarding data inaccuracy reporting procedures, compliance processes, and how compliance is to be enforced within the ARDS-Registry-Registrar-Registrant loop.

The EWG states that having the IP address of the registrant[19] available would facilitate "abuse mitigation." That data would aid some investigators and therefore fulfill their purposes. But what are missing are policy and security justifications for that purpose and potentially making that data available. Does the purpose of "abuse mitigation" justify giving additional parties access to sensitive data, how does one define allowable parties, is it possible in the context of data protection laws, and can it be executed in a secure and responsible fashion?

In any case, the SSAC believes it is vital that security responders and researchers continue to have access to domain contact data where allowed by law. They generally should not be given less access to registration data than they are afforded now, nor should they be charged in the future for the access they currently have now.

3. Recommendations

Recommendation 1: SSAC reiterates its recommendation from SAC055: The ICANN Board should explicitly defer any other activity (within ICANN's remit) directed at finding a 'solution' to 'the WHOIS problem' until the registration data policy has been developed and accepted in the community. The EWG should clearly state its proposal for the purpose of registration data, and focus on policy issues over specific implementations.

Specifically, SSAC does not believe the EWG has answered the question of the purpose of registration data. A clear statement of the purpose is essential before a thorough and

[18]The EWG addressed proxy registrations and "at-risk" registrants, such as those who fear for their lives. EWG Draft report, section "VI. Addressing Privacy Concerns," page 33.

[19] This means the IP address from which the domain registration was made, not the A record(s) of the domain name.

complete risk analysis can be completed of the proposed next generation directory services.

Recommendation 2: The ICANN Board should ensure that a formal security risk assessment of the registration data policy be conducted as an input into the Policy Development Process.

A separate security risk assessment should also be conducted regarding the implementation of the policy.

Recommendation 3: SSAC recommends that the EWG state more clearly its positions on the following questions of data availability:

A. Why is a change to public access justified? This explanation should describe the potential impact upon ordinary Internet users and casual or occasional users of the directory service.

B. Does the EWG believe that access to data currently accessible in gTLD WHOIS output should become restricted? If so, what fields, and to what extent exactly? Under the EWG proposal, queries from non-authenticated requestors would return only "public data available to anyone, for any purpose".[20] At this time it is unspecified what the set of "public data available to anyone" is, and therefore it is unclear if the infrequent or non-professional users will lose access to data they rely upon, when they need it. It appears that Annex C may recommend that non-authenticated users be denied access to several data elements that they can access today via WHOIS. Annex C also neglects to mention Administrative, Technical, and Billing contacts. Will access to a currently public source of data be degraded and made less useful for a large number of users so that a smaller number of users can receive enhanced access, and if so why is such a shift justified?

C. Should all gTLD registries be required to provision their contact data into the ARDS? There are jurisdictions that prohibit by law the export of personally identifiable information outside the jurisdiction. As a result, the ARDS may not be a viable way to deliver data accuracy and compliance across all gTLDs.[21]

[20] See EWG Initial Report, page 35.

[21] See European Parliament and the Council (2002). Directive on Privacy and electronic communications. (2002/58/EC) Retrieved from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML; European Parliament and Council (1995). Directive on the protection of individuals with regard to the processing of persona data and on the free movement of such data (95/46/EC). Retrieved from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

D. Does the EWG propose more types of sensitive registration data be provisioned into ARDS than are found in current gTLD WHOIS output? This question was left unanswered in Annex C. Proposals to do so should be justified.

   a. For example, the EWG listed the IP address of the registrant as a type of registration data.[22] Does the EWG propose that this data be provisioned by registrars to the registries, and then from the registries into the ARDS and made available to those parties with a need to perform the stated purpose of "Abuse Mitigation"? In such cases, the EWG needs to demonstrate a justification that goes beyond saying that the provisioning of such data would "serve the purpose" of certain data consumers. Instead, the question is whether giving additional parties access to such data is a good idea, and how it might be justified.

   b. The EWG also listed "EPP Transfer Key" as a type of registration data. We assume this is the EPP auth_info code for a domain. The provisioning of EPP auth_info codes into a meta-registry poses a major security risk and should never be allowed.

Recommendation 4: The SSAC suggests that the EWG address this recommendation from SAC058: "SSAC Report on Domain Name Registration Data Validation".[23]

As the ICANN community discusses validating contact information, the SSAC recommends that the following meta-questions regarding the costs and benefits of registration data validation should be answered:

- *What data elements need to be added or validated to comply with requirements or expectations of different stakeholders?*
- *Is additional registration processing overhead and delay an acceptable cost for improving accuracy and quality of registration data?*
- *Is higher cost an acceptable outcome for improving accuracy and quality?*

[22] See EWG Initial Report, page 45.
[23] See SSAC Report on Domain Name Registration Data Validation (27 March 2013) at http://www.icann.org/en/groups/ssac/documents/sac-058-en.pdf.

- *Would accuracy improve if the registration process were to provide natural persons with privacy protection upon completion of multi-factored validation?*
- *Would any single central authority be equipped to make authentication and authorization judgments pertaining to access to registration data?*

4. Acknowledgements, Statements of Interests, and Objections, and Withdrawals

In the interest of greater transparency, these sections provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent, or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

4.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this Report.

SSAC Members:

Greg Aaron
Jeff Bedser
Don Blumenthal
Jim Galvin
Sarmad Hussain
Merike Kaeo
Doron Shikmoni

Staff:
Barbara Roseman
Julie Hedlund
Steve Sheng (editor)

4.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/committees/security/biographies-25mar11-en.htm.

4.3 Objections and Withdrawals

There were no objections. There were the following withdrawals:

KC Claffy
Rod Rasmussen