

SAC124
SSAC Advice on Name Collision Analysis

Preface

In this document the Security and Stability Advisory Committee (SSAC) provides its analysis of the findings and recommendations presented within the Name Collision Analysis Project (NCAP) Study Two and the proposed Name Collision Risk Assessment Framework. The SSAC also provides additional commentary on several aspects of the NCAP Study Two Report and makes recommendations to the ICANN Board.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., 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 authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any dissenting opinions or alternative views that are included at the end of the document.

Table of Contents

Executive Summary	4
1 Introduction	6
2 SSAC’s View on the Findings and Recommendations of NCAP Study Two	7
2.1 Timing of Name Collision Assessment and Mitigation	8
3 Additional Findings by the SSAC	8
3.1 Privacy risks are an inherent part of managing the broader risk of name collisions	9
3.2 Avoiding Data Collection over Privacy Concerns Amounts to Risk Transfer and May Amplify Potential for Privacy Harm	11
3.3 Prioritize finding solutions that allow for sufficient data collection and analysis to properly inform mitigation strategies	12
4 Recommendations	13
5 Acknowledgments, Statements of Interest and Withdrawals	13
5.1 Acknowledgments	14
5.2 Statements of Interest	15
5.3 Withdrawals	15

Executive Summary

The ICANN Security and Stability Advisory Committee (SSAC) recognizes and applauds the significant volunteer efforts that contributed to the development of the Name Collision Analysis Project (NCAP) Study Two report.

The SSAC fully endorses the findings and recommendations presented in NCAP Study Two report¹ and recommends that the ICANN Board adopt and implement these recommendations. The SSAC supports the centralized and coordinated approach proposed by the NCAP Study Two. This approach is essential for implementing effective measures to mitigate the two data-access-related risks associated with name collisions. These risks differ based on who has access to sensitive data exposed by name collisions and their obligations towards handling exposed data:

- **Delegation Risk:** Privacy and risks to users and end systems from name collisions associated with the delegation of a top-level domain (TLD)
- **Assessment Risk:** Privacy risks associated with the execution of data collection methods in the proposed Name Collision Risk Assessment Framework (“Proposed Framework”).

The SSAC acknowledges ICANN org’s privacy concerns surrounding the proposed data collection methods discussed in Section 3 of NCAP Study Two report and the legal memo submitted by ICANN org to the Public Comment proceeding on the draft of Study Two report.² The SSAC offers the following three considerations:

1. Privacy risks are inherent in managing the broader risk of name collisions. ICANN's role in coordinating the allocation and assignment of generic top-level domains (gTLDs) necessitates some level of data collection in order to make informed decisions about delegating strings with name collision risks.
2. Avoiding data collection does not resolve privacy risks related to name collisions; rather, it transfers these risks onto third parties, potentially leading to more significant impact on privacy overall.
3. Effectively managing Security, Stability and Resiliency (SSR) risks in the context of name collisions requires a proactive approach towards name collision identification and mitigation.

Based on these considerations, the SSAC recommends that the ICANN Board prioritize finding solutions within the Proposed Framework that allow for sufficient data collection and analysis to properly inform mitigation strategies for name collisions.

¹ ‘Name Collision Analysis Project Study Two Report’. ICANN Name Collision Analysis Project Discussion Group, 5 April 2024. <https://www.icann.org/en/system/files/files/ncap-study-2-report-05apr24-en.pdf>.

² ICANN Org’s public comment to NCAP Study Two draft report, <https://www.icann.org/en/public-comment/proceeding/ncap-study-2-draft-report-01-19-2024/submissions/icann-org-26-02-2024>

Failing to properly mitigate Delegation Risk due to concerns about Assessment Risk for ICANN (or other mitigating parties) would be a strategic mistake. Risks to users and end systems from name collisions associated with the delegation of a TLD directly threaten the security and stability of the domain name system (DNS), its dependent systems, and, ultimately, end-user privacy. Mitigating these risks aligns with ICANN's mission and serves the best interests of the global internet community. Assessment Risk, when appropriately minimized and weighed against the benefits of mitigating Delegation Risk, is a necessary trade-off to ensure the stable and secure operation of the DNS.

To this end, the SSAC makes the following recommendations:

Recommendation 1: The SSAC recommends that the ICANN Board adopt and implement all the recommendations in NCAP Study Two.

Recommendation 2: The SSAC urges the ICANN Board to prioritize finding appropriate solutions within the proposed Name Collision Risk Assessment Framework that allow for sufficient data collection and analysis to properly inform mitigation strategies for name collisions.

Recommendation 3: The SSAC welcomes the engagement from ICANN Org and is committed to offer its expertise throughout the process.

1 Introduction

In this advisory, the SSAC provides its advice on name collision analysis based on the Name Collision Analysis Project (NCAP) Discussion Group Study Two report.

The ICANN Board tasked the SSAC in resolutions 2017.11.02.29 – 2017.11.02.31 to address questions related to name collisions.³ To fulfill the Board’s request, the SSAC chartered the NCAP and developed three studies to answer the Board’s questions. The ICANN Board authorized Study One in March 2019, and the NCAP Discussion Group published Study One in July 2020.⁴ Based on the findings and recommendations of Study One, the NCAP Discussion Group revised the Study Two proposal.⁵ The ICANN Board authorized Study Two in resolutions 2021.03.25.11-2021.03.25.14, and the NCAP Discussion Group completed Study Two in April 2024.^{6,7}

Study Two contained the main report, detailed responses to Board Resolution 2017.11.20.30, a case study of collision strings, a perspective study of domain name system (DNS) queries for non-existent top-level domains (TLDs), a root cause analysis of wpad.domain.name, and a root cause analysis of new generic top-level domain (gTLD) collisions reported to ICANN.^{8,9,10,11,12,13}

³ ‘Approved Board Resolutions | Regular Meeting of the ICANN Board: Consideration of .CORP, .HOME, and .MAIL and Other Collision Strings’, 2 November 2017.
<https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-regular-meeting-of-the-icann-board-02-11-2017-en#2.a>.

⁴ Scarfone, Karen. ‘Managing the Risks of Top-Level Domain Collisions’. ICANN Name Collision Analysis Project Discussion Group, 19 June 2020. <https://www.icann.org/en/system/files/files/ncap-study-1-report-19jun20-en.pdf>.

⁵ The NCAP Discussion Group includes individual participants from the SSAC as well as individual participants from across the ICANN community

⁶ ‘Approved Board Resolutions | Regular Meeting of the ICANN Board: Accepting Name Collision Analysis Project (NCAP) Study 1 and Proceeding with Study 2’, 25 March 2017.
<https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-regular-meeting-of-the-icann-board-25-03-2021-en#2.b>.

⁷ ‘Name Collision Analysis Project Study Two Report’. ICANN Name Collision Analysis Project Discussion Group, 5 April 2024. <https://www.icann.org/en/system/files/files/ncap-study-2-report-05apr24-en.pdf>.

⁸ ‘Name Collision Analysis Project Study Two Report’.
<https://www.icann.org/en/system/files/files/ncap-study-2-report-05apr24-en.pdf>

⁹ ‘Responses to Board Resolution 2017.11.02.30 by the Name Collision Analysis Project Discussion Group’. ICANN Name Collision Analysis Project Discussion Group, 5 April 2024.
<https://www.icann.org/en/system/files/files/board-responses-ncap-dg-05apr24-en.pdf>.

¹⁰ ‘Case Study of Collision Strings’. ICANN Name Collision Analysis Project Discussion Group, 13 July 2022.
<https://www.icann.org/en/system/files/files/case-study-collision-strings-13jul22-en.pdf>.

¹¹ ‘A Perspective Study of DNS Queries for Non-Existent Top-Level Domains’. ICANN Name Collision Analysis Project Discussion Group, 13 July 2022.
<https://www.icann.org/en/system/files/files/perspective-study-dns-queries-non-existent-top-level-domains-13jul22-en.pdf>.

¹² Deccio, Casey. ‘Root Cause Analysis - Wpad.Domain.Name’. ICANN Name Collision Analysis Project Discussion Group, 18 January 2023.
<https://www.icann.org/en/system/files/files/root-cause-analysis-wpad-18jan23-en.pdf>.

¹³ Deccio, Casey. ‘Root Cause Analysis - New GTLD Collisions’. ICANN Name Collision Analysis Project Discussion Group, 18 January 2023.
<https://www.icann.org/en/system/files/files/root-cause-analysis-new-gtld-collisions-18jan23-en.pdf>.

The SSAC commends the dedication and expertise demonstrated by the community in producing these reports. The NCAP Discussion Group held a total of 142 teleconferences that were open to the community, produced three public consultations on various reports, and held open discussions with the community at over ten ICANN public meetings.¹⁴ The SSAC also commends ICANN org’s support of the project, led by the Office of the Chief Technology Officer (OCTO). The SSAC especially appreciates ICANN org’s public input to the public comment proceedings of various Study Two reports. The meticulous research and collaborative spirit evident in the work are crucial in tackling the multifaceted issue of name collisions.

2 SSAC’s View on the Findings and Recommendations of NCAP Study Two

The SSAC fully endorses the findings and recommendations of NCAP Study Two. The report’s findings are comprehensive and insightful. They shed light on various aspects of name collisions, providing a nuanced view of the challenges and potential risks. We believe they resonate with the guidance provided in our previous advisories, particularly SAC062 and SAC066.^{15,16}

In particular, the SSAC appreciates that NCAP’s proposal emphasizes risk management, consistent definitions, and proactive measures. NCAP Study Two’s emphasis on treating name collisions as a risk management problem is particularly noteworthy. This perspective is crucial for understanding acceptable risk levels and informing effective risk assessment and mitigation strategies. Equally important is the call for a consistent definition of name collisions. A clear and uniform understanding is fundamental for accurately assessing risks and determining the scope of concern.

The SSAC strongly endorses Study Two’s recommendation to temporarily delegate strings for risk assessment before granting a string to an applicant. This approach aligns with our previous advice¹⁷ and is critical for understanding the entire risk spectrum of name collisions and their impact. We strongly advocate for the establishment of a dedicated Technical Review Team (TRT) and the more comprehensive Name Collision Risk Assessment Framework¹⁸ (“Proposed Framework”) to replace the existing Name Collision Occurrence Management Framework (“Current Framework”).¹⁹ These measures will enable a more thorough and adaptive response to the evolving nature of name collisions and the diverse needs of the internet ecosystem.

¹⁴ SSAC Name Collision Analysis Project (NCAP) Home. ‘SSAC Name Collision Analysis Project (NCAP) Home’, <https://community.icann.org/display/NCAP/SSAC+Name+Collision+Analysis+Project+%28NCAP%29+Home>.

¹⁵ SAC062: SSAC Advisory Concerning the Mitigation of Name Collision Risk, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-062-en.pdf>

¹⁶ SAC066: SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-066-en.pdf>

¹⁷ See SAC062 and SAC066

¹⁸ ‘Name Collision Occurrence Management Framework’. ICANN, 30 July 2014. <https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf>.

¹⁹ See Appendix 3: Name Collision Risk Assessment Framework, ‘Name Collision Analysis Project Study Two Report’.

2.1 Timing of Name Collision Assessment and Mitigation

NCAP Study Two identifies security and privacy risks associated with name collisions for users and end systems when delegating a TLD string to the DNS root (“delegation risks”). Proactive measures are essential to assess and mitigate delegation risks. The critical question is *when* and *where* to implement these measures. Table 1 below summarizes the key elements of the Current Framework vs. the Proposed Framework.

The SSAC believes the Proposed Framework is more appropriate than the Current Framework because a centralized, coordinated approach to assess and mitigate name collision ensures the consistency and overall effectiveness of the effort to safeguard the secure expansion of the internet's namespace. A decentralized approach that relies on registries to address these complex technical challenges is not ideal, given their varied capabilities and incentives.

Table 1: Comparison of Name Collision Assessment and Mitigation between the Current Framework and the Proposed Framework

	Current Framework	Proposed Framework
Name Collision Assessment	<ul style="list-style-type: none"> - ICANN uses root server data to assess name collisions. - ICANN considers .home, .corp, .mail high risk and deferred delegation indefinitely. 	<ul style="list-style-type: none"> - ICANN makes name collisions visible through temporary delegation. - TRT uses data made available through temporary delegation to assess name collision risks on a per-string basis. - The ICANN Board uses the TRT’s recommendations as an input in its decision to grant the TLD.
Name Collision Mitigation and Notification	<ul style="list-style-type: none"> - Mitigation & notification is <i>done by TLD operators after the granting and delegation of the TLD.</i> - TLD registry operators execute controlled interruption for 90 days after delegation. - TLD operators respond to name collision reports by ICANN within two hours for two years. 	<ul style="list-style-type: none"> - Notification is done <i>by ICANN prior to granting the TLD.</i> - Notification methods include controlled interruption (CI) or visible interruption with notification (VIN). - Mitigation or remediation strategies are developed by the applicant and assessed for efficacy by the TRT <i>prior</i> to granting the TLD.

3 Additional Findings by the SSAC

NCAP Study Two’s proposed name collision data gathering and assessment methods are required to provide the ICANN Board with actionable information to evaluate and assess these risks per TLD and to properly inform applicants when developing mitigation or remediation strategies.

The SSAC understands that as these tools are deployed and utilized to collect data, it is crucial to carefully examine and address any potential privacy risks that may manifest with the data collected.

Regarding privacy concerns, SSAC offers the following three considerations:

1. Privacy risks are inherent in managing the broader risk of name collisions. ICANN's role in coordinating the allocation and assignment of gTLDs necessitates some level of data collection in order to make informed decisions about delegating strings with name collision risks.
2. Avoiding data collection does not resolve privacy risks related to name collisions; rather, it transfers these risks onto third parties, potentially leading to more significant harm to privacy overall.
3. Effectively managing security, stability, and resiliency (SSR) risk in name collisions requires a proactive approach towards name collision identification and mitigation. The ICANN Board should prioritize finding solutions that do not compromise on critical SSR objectives while addressing privacy concerns.

The following sections expand on each of these considerations.

3.1 Privacy risks are an inherent part of managing the broader risk of name collisions

NCAP Study Two asserts, and SSAC concurs, that name collisions pose well-documented SSR and privacy risks to the internet's infrastructure and end users. Effectively managing name collisions requires a balanced approach to risk management. The SSAC identifies two main types of privacy risks concerning name collision management:

- **Delegation Risk:** Privacy risks to users and end systems from name collisions associated with the delegation of a TLD
- **Assessment Risk:** Privacy risks associated with the execution of the Proposed Framework

While both delegation risk and assessment risk involve potential exposure of sensitive data due to name collisions, the distinction lies in who has access to exposed data and their obligations towards data handling. Delegation risk arises when a name collision occurs during the normal operation of the DNS, exposing data to potentially unknown actors. The data could be intercepted by malicious parties or inadvertently leaked by a misconfigured server. Assessment risk, on the other hand, involves a controlled process where a designated entity actively investigates name collisions. According to the Proposed Framework, this designated entity would be obligated to implement safeguards to protect the privacy of the user data.

It's crucial to understand that the privacy concerns in the assessment risk are an inherent part of managing the broader delegation risk of name collisions. Today's complex Internet infrastructure makes it difficult to identify name collisions. To address this challenge, we need methods to

make these collisions more visible— this entails some risk. However, proper assessment would lead to the design of more effective mitigation methods. The utility and benefits of effective mitigation methods lie in their ability to reduce the delegation risk. Thus, the ICANN Board must weigh the assessment risks against the assessments’ effectiveness in reducing the delegation risk.

Furthermore, prior data collection methods underestimate delegation risks in the current landscape. The adoption of new DNS protocol enhancements (e.g., query name minimization, aggressive NSEC caching) makes much less information available at root servers. Given these technological advancements and differing data anonymization techniques applied by root server operators, root-server data alone is insufficient to properly identify and assess the delegation risks of name collisions. Therefore, making name collisions visible through temporary delegation of the TLD is crucial for proper assessment.

The last decade also saw major adoption of IPv6. However, controlled interruption as implemented in 2012 does not work for IPv6-only clients. The Proposed Framework offers better ways to notify the affected systems and end users.

The SSAC acknowledges ICANN org’s privacy concerns surrounding the data collection methods, particularly for Visible Interruption (VI) and Visible Interruption with Notification (VIN). The SSAC does not advocate ignoring the assessment risks but emphasizes the dangers of neglecting the delegation risks altogether. ICANN’s role in coordinating the allocation and assignment of gTLDs necessitates some level of data collection in order to make informed decisions about delegating strings with delegation risks. Entirely avoiding data collection severely limits ICANN’s ability to assess and mitigate name collision impacts.

While visible interruption (or visible interruption with notification) discloses more data than controlled interruption, without effective mitigation, this data will also be disclosed once a TLD is available for registration. Furthermore, without adequate mitigation, malicious parties can intentionally register names to access sensitive information resulting from name collisions. The Proposed Framework manages these risks by having trusted parties make the name collisions visible through temporary delegation, properly assessing the risk associated with identified name collisions, and mitigating these risks. To address privacy concerns, NCAP Study Two proposes only logging data necessary for identifying, assessing, and mitigating name collisions on a per-string basis.

Failing to fully mitigate delegation risks due to concerns about assessment risks for ICANN (or other mitigating parties) would be a strategic mistake. Delegation risks directly threaten the security and stability of the DNS, its relaying systems, and, ultimately, end-user privacy. Mitigating these risks aligns with ICANN’s mission and serves the best interests of the global internet community. Assessment Risk, when appropriately minimized and weighed against the benefits of mitigating Delegation Risk, is a necessary trade-off to ensure the stable and secure operation of the DNS.

3.2 Avoiding Data Collection over Privacy Concerns Amounts to Risk Transfer and May Amplify Potential for Privacy Harm

Avoiding data collection does not resolve the delegation risk related to name collision; rather, it transfers these delegation risks onto third parties (e.g., TLD operators or registrants). In addition, a decentralized execution of the Proposed Framework could inadvertently increase the privacy harm to end users. The data that is generated or shared because of name collisions – in the Current Framework, the data ICANN did not collect and did not have available as part of the assessment phase– would still be generated by activities using the colliding gTLD names, but would surface under different conditions, to different observers with different obligations. This is not a recommended path forward for at least four reasons:

First, third parties (e.g., TLD operators) may lack the incentive, data, or tools to properly evaluate and mitigate name collision risks, including the privacy risks inherent in name collisions more broadly. This could leave sensitive information potentially being collected or compromised as a side effect of leaving that evaluation and mitigation undone. Due diligence assessments and contractual requirements by ICANN would fall short of real-time monitoring and mitigation - ICANN's actions would necessarily be after adverse impacts have occurred if the risk assessment is transferred to TLD operators.

Second, without effective mitigation, once a TLD is available for registration, malicious parties could intentionally register names to gain access to sensitive information resulting from name collisions.

Third, transferring mitigation to multiple (willing and capable) third parties introduces barriers to coordination and knowledge transfer and complicates what is already a highly complex technical and operational task. As a result, each of these parties may make different decisions with respect to data gathering and assessment methods employed and may arrive at inconsistent conclusions.

Fourth, an important element of the Proposed Framework is to notify system administrators and end users who use domains that collide with a soon-to-be granted gTLD. Such notifications provide awareness and incentives for system administrators and end users to reconfigure their systems, addressing name collision risks at the core. Since ICANN is the global coordination entity, notification systems centrally managed and implemented by ICANN would be more trustworthy than a patchwork of notification systems implemented by various third parties.

An approach that avoids data collection for the express and sole purpose of mitigating assessment risk is detrimental to ICANN's mission of ensuring the stable and secure operation of the Internet's unique identifier systems. Few actors are better positioned than ICANN to justify mitigation and its associated minimized processing of personal data (or personally identifiable information) in the public interest and the interest of the wider community.

3.3 Prioritize finding solutions that allow for sufficient data collection and analysis to properly inform mitigation strategies

The SSAC acknowledges the assessment-related privacy concerns with the data collection methods in the Proposed Framework. However, we caution against prioritizing Assessment Risk at the expense of the more significant Delegation Risk posed by name collisions themselves. Effectively managing SSR risks in the context of name collisions requires a proactive approach towards name collision identification, risk assessment, and mitigation.

It's crucial to remember that some level of risk is unavoidable. NCAP Study Two Recommendation 1 aptly states that "ICANN should treat name collisions as a risk management problem." The SSAC advises the ICANN Board to prioritize mitigating the known delegation risks associated with name collisions, as outlined in NCAP Study Two.

Fortunately, many assessment-related privacy risks may be mitigated preemptively without compromising their efficacy. NCAP Study Two provides information for a Data Protection Impact Assessment (DPIA) and data minimization practices, with descriptions of data processed in each assessment method. Moreover, in line with privacy by design, the principles of proportionality and subsidiarity should guide the TRT when it selects appropriate assessment methods and the order in which they are utilized to perform assessment. While some of the proposed assessment methods are new to ICANN, operational experience with "honeypots" demonstrates that clear data policies and protocols can manage privacy risks. In these environments, policies state (1) the data that is collected, the purpose that the data is gathered for, who the data is shared with and how long the data is retained; (2) processes and operational procedures to minimize the data collected, to protect the collected data and (3) justification of legitimate interest for the company to collect the data which does not override the rights of the data subject. Recital 49 of the European Union General Data Protection Regulation (GDPR) "Network and Information Security as Overriding Legitimate Interest" provides grounds for the collection of data for network information security purposes. In addition, there are known Sinkhole operators such as Shadowserver/Registry of Last Resort and efforts like the Conficker Working Group that have done this in the past and their experience would be instructive.²⁰

Should the ICANN Board decide not to adopt the Proposed Framework, it must explicitly communicate the transfer of risk to third parties, so that they can make informed risk assessments and mitigation decisions.

In conclusion, the SSAC urges ICANN to prioritize finding solutions within the Proposed Framework that allow for sufficient data collection and analysis to properly inform mitigation strategies for name collisions.. This prioritization aligns with ICANN's mission to ensure the stable and secure operation of the Internet's unique identifier systems.

²⁰ See, for example, the Shadowserver EU privacy statement available at: <https://www.shadowserver.eu/privacy.en.html>

4 Recommendations

Recommendation 1: The SSAC recommends that the ICANN Board adopt and implement the recommendations in NCAP Study Two.

Recommendation 2: The SSAC urges the ICANN Board to prioritize finding appropriate solutions within the proposed Name Collision Risk Assessment Framework that allow for sufficient data collection and analysis to properly inform mitigation strategies for name collisions.

The SSAC acknowledges there are privacy risks associated with collecting data necessary for the assessment methods in the Proposed Framework and notes that such risks are inherent in managing the broader risk of name collisions. However, the SSAC believes Assessment Risk, when properly minimized, pose less harm to end users and systems than the broader Delegation Risks stemming from unmitigated, or under mitigated, name collisions.

A robust framework, such as the Proposed Framework, empowers the ICANN Board with the necessary data to make informed decisions on high-risk string delegations. This, in turn, allows for the development of mitigation strategies that target the root causes of name collisions for each specific string. Ultimately, such a data-driven approach should sufficiently equip the ICANN Org and the ICANN Board to ensure the continued stability and security of the DNS in the next round of New gTLDs.

Recommendation 3: The SSAC welcomes the engagement from ICANN Org and is committed to offer its expertise throughout the process.

The SSAC acknowledges that neither the NCAP Study 2 Report, nor this advisory provides an exhaustive treatment on privacy aspects of managing name collisions issues. We look forward to continuing to build on this work in a collaborative manner with ICANN Org and other privacy experts.

5 Acknowledgments, Statements of Interest and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Statements of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member’s participation in the preparation of this Report. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this report is concerned. Except for members listed in the Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

5.1 Acknowledgments

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

SSAC Members

Maarten Aertsen
Jaap Akkerhuis
Patrik Fältström
James Galvin
Merike Kåo
Warren Kumari
Barry Leiba
Ram Mohan
Russ Mundy
Rod Rasmussen
Matthew Thomas
Tara Whalen
Suzanne Woolf

ICANN staff

Steve Sheng (editor)
Danielle Rutherford (editor)
Moses Baguma
Kathy Schnitt

The committee also wishes to thank the extraordinary effort of the cross-community volunteers and ICANN support staff in the NCAP Discussion Group for their time, contributions, and review in producing NCAP Study Two.

NCAP Study Two Discussion Group Members

Anne Aikman-Scalese
Jaap Akkerhuis*
Thomas Barrett
Dmitry Belyavsky
Justine Chew
Steve Crocker*
Patrik Fältström* (Co-Chair, 1 April 2020—30 September 2021)
Betty Fausta
James Galvin* (Co-Chair, 1 April 2020—17 November 2022)
Julie Hammer*
Merike Kåo*
Rubens Kühl

SSAC Advice on Name Collision Analysis

Warren Kumari*
Barry Leiba*
Danny McPherson*
Brantly Millegan
Ram Mohan*
Russ Mundy*
Jeff Neuman
Eric Osterweil
Rod Rasmussen*
Chris Roosenraad*
Jeff Schmidt
Greg Shatan
Matthew Thomas* (Co-Chair, 1 April 2020—5 April 2024)
Suzanne Woolf* (Co-Chair, 30 November 2022—5 April 2024)

*SSAC member

ICANN Support

Jennifer Bryce
Casey Deccio (Researcher)
Heather Flanagan (Technical Writer)
Kinga Kowalczyk
Matt Larson
Jonathan Phillips
Michael Puckett (Technical Writer)
Karen Scarfone (Technical Writer)
Kathy Schnitt
Steve Sheng

5.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at:

<https://www.icann.org/en/ssac/members>

NCAP Discussion Group member Disclosure of Interest are available at:

<https://community.icann.org/display/NCAP/NCAP+Discussion+Group>

5.3 Withdrawals

There were no withdrawals.