ICANN BOARD PAPER NO. 2021.07.22.1b

TITLE: **Security and Stability Advisory Committee (SSAC) Member Appointments**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

The Security and Stability Advisory Committee (SSAC) recommends the Board reappoint the SSAC members as identified in the proposed resolution, and respectfully requests the appointment of Russ Housley, Jonathan Spring, and Jiankang Yao as new Committee members.

COMMITTEE RECOMMENDATION:

The Committee desires two actions from the ICANN Board: 1) the reappointment of the SSAC members as identified in the proposed resolution, and 2) the appointment of Russ Housley, Jonathan Spring, and Jiankang Yao to the SSAC.

PROPOSED RESOLUTION:

Whereas, the Board, at Resolution 2010.08.05.07 approved Bylaws revisions that created three-year terms for SSAC members, required staggering of terms, and obligated the SSAC Chair to recommend the reappointment of all current SSAC members to full or partial terms to implement the Bylaws revisions.

Whereas, in January 2021 the SSAC Membership Committee initiated an annual review of nine SSAC members whose terms are ending 31 December 2021 and submitted to the SSAC its recommendations for reappointments on 11 June 2021.

Whereas, on 18 June 2021, the SSAC members approved the reappointments.

Whereas, the SSAC recommends that the Board reappoint the following SSAC members to three-year terms: Jaap Akkerhuis, Patrik Fältström, Ondrej Filip, Jim Galvin, Robert Guerra, Julie Hammer, Ram Mohan, Doron Shikmoni and Suzanne Woolf.

Whereas, the SSAC Membership Committee, on behalf of the SSAC, requests that the Board should appoint Russ Housley, Jonathan Spring, and Jiankang Yao to the SSAC for terms beginning immediately upon approval of the Board and ending on 31 December 2024.

Resolved (2021.07.22.xx), the Board accepts the recommendation of the SSAC and reappoints the following SSAC members to three-year terms beginning 01 January 2022 and ending 31 December 2024: Jaap Akkerhuis, Patrik Fältström, Ondrej Filip, Jim Galvin, Robert Guerra, Julie Hammer, Ram Mohan, Doron Shikmoni and Suzanne Woolf.

Resolved (2021.07.22.xx), that the Board appoints Russ Housley, Jonathan Spring, and Jiankang Yao to the SSAC for terms beginning immediately upon approval of the Board and ending on 31 December 2024.

PROPOSED RATIONALE:

The SSAC is a diverse group of individuals whose expertise in specific subject matters enables the SSAC to fulfill its role and execute its mission. Since its inception, the SSAC has invited to its membership individuals with deep knowledge and experience in technical and security areas that are critical to the security and stability of the Internet's naming and address allocation systems.

The SSAC's continued operation as a competent body is dependent on the accumulation of talented subject matter experts who have consented to volunteer their time and energies to the execution of the SSAC mission.

Russ Housley is the founder and owner of Vigil Security, LLC which provides computer and networking security consulting services. He is a recognized expert in security protocols, system engineering and system security architectures and brings significant knowledge and skills in cryptography. He has chaired the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB) and has authored or contributed to many Internet standards. Russ served as an SSAC endorsed member of the SSR2 Review Team from June 2018 and was appointed by the Team as its chair.

Jonathan Spring is a member of the Technical Staff, Computer Emergency Response Team Coordination Centre (CERT/CC) of the Software Engineering Institute, Carnegie Mellon University. He has expertise and experience in incident response and Computer Security Incident Response Team (CSIRT) practices, network and DNS traffic analysis for detecting incidents, situational awareness for contextualizing such incidents, and vulnerability management for reducing incidents. He participates in the Forum of Incident Response and Security Teams (FIRST) and was a SSAC Research Fellow from 2014-2016.

Jiankang Yao is a research engineer with China Internet Network Information Centre (CNNIC), with his main research interests including Email Address Internationalization (EAI), Internationalized Domain Names (IDN), DNS, Internet naming and addressing. He participates in IETF work, is a member of the IAB, was appointed to the ccNSO Council with effect March 2021, and serves as the Co-Secretary of the Chinese Domain Name Consortium (CDNC).

This resolution is an organizational administrative function for which no public comment is required. The appointment of SSAC members is in the public interest and in furtherance of ICANN's mission as it contributes to the commitment of the ICANN to strengthen the security, stability, and resiliency of the DNS. The appointment of SSAC members is not anticipated to have any fiscal impact on ICANN org that has not already been accounted for in the budgeted resources necessary for ongoing support of the SSAC.

Signature Block:

Submitted by:	Merike Kaeo
Position:	Liaison to the ICANN Board from the Security and Stability Advisory Committee
Date Noted:	30 June 2021
Email:	merike.kaeo@board.icann.org

ICANN BOARD SUBMISSION No. 2021.07.22.1c

TITLE:	**Transfers to Reserve Fund and Supplemental Fund for Implementation of Community Recommendations**
PROPOSED ACTION:	**For Board Consideration and Approval**

EXECUTIVE SUMMARY:

The Board is being asked to approve a transfer to the Reserve Fund and an initial transfer to the Supplemental Fund for Implementation of Community Recommendations (SFICR) from the Operating Fund.

Per the ICANN Investment Policy (ICANN Investment Policy), the Operating Fund is set at a target level necessary to fund a minimum of three months expected operating expenses. Then, the Reserve Fund must be at or above its target level, equivalent to one year of budgeted operating expenses, to ensure financial sustainability and resilience to unforeseen events. Finally, the SFICR can be allocated funds as is deemed useful to support increasing the capacity of the organization to address projects that are multi-year and focus on community recommendations that are approved or soon to be adopted by the Board but cannot fit within the annual budget.

In May 2021, the Board approved a US$10,000,000 transfer from the Operating Fund to the Reserve Fund. With the remaining excess above the target level in the Operating Fund, currently estimated to be about US$38,000,000, ICANN organization recommends that US$5,000,000 be transferred to the Reserve Fund and an initial amount of US$15,000,000 be transferred to the SFICR. The remaining excess after those transfers will be addressed with the Board via a proposed Investment Policy update.

ICANN ORGANZATION AND BOARD FINANCE COMMITTEE (BFC) RECOMMENDATIONS *(Subject to BFC Approval)*:

Both ICANN organization and the BFC recommend that the Board approve:

- The transfer of US$5,000,000 from the Operating Fund to the Reserve Fund
- The transfer of US$15,000,000 from the Operating Fund to the SFICR

PROPOSED RESOLUTION:

Whereas, the Operating Fund includes the funds used for ICANN's day-to-day

operations and must contain enough funds to cover a minimum of three months of ICANN organization's operating expenses.

Whereas, periodically, excess funds in the Operating Fund may be transferred to the Reserve Fund to ensure its balance is at or above the minimum target level, as determined and approved by the Board.

Whereas, a Supplemental Fund for Implementation of Community Recommendations (SFICR) will allow ICANN to segregate resources in support of increasing the capacity of the organization to address projects that are multi-year and focus on community recommendations that are approved or soon to be adopted by the Board but cannot fit within the annual budget.

Whereas, periodically, if excess funds exist in the Operating Fund after an allocation to the Reserve Fund has been considered or decided, an allocation to the SFICR will be considered based on the project needs identified.

Whereas, ICANN organization has determined that the balance of the Operating Fund as of 31 May 2021, based on unaudited Financial Statements, contained excess funds.

Whereas, both ICANN organization and the Board Finance Committee have recommended that the Board approve a US$5,000,000 transfer to the Reserve Fund and a US$15,000,000 transfer to the SFICR from the Operating Fund.

Resolved (2021-07-22-xx), the Board approves the transfer of US$5,000,000 from the Operating Fund to the Reserve Fund.

Resolved (2021-07-22-xx), the Board approves the transfer of US$15,000,000 from the Operating Fund to the SFICR.

PROPOSED RATIONALE:

As part of ICANN's Investment Policy, the Operating Fund should be at a level of funds to cover a minimum of three months of ICANN organization's operating expenses, and that any amount determined to be in excess may be transferred to the Reserve Fund to ensure its balance is at or above the minimum target level, as determined and approved by the Board.

The Supplemental Fund for Implementation of Community Recommendations (SFICR) establishes segregated resources in support of increasing the capacity of the organization to address activities projects that are multi-year and focus on community recommendations that are approved or soon to be adopted by the Board but cannot fit within the annual budget. If the Operating Fund contains excess after an allocation to the Reserve Fund has been considered or decided, an allocation to the SFICR will be determined based on the project needs identified.

ICANN organization has evaluated the balance of the Operating Fund as of 31 May 2021 on the basis of its unaudited Financial Statements and has determined that excess funds of US$5,000,000 should be transferred to the Reserve Fund and US$15,000,000 should be transferred to the SFICR.

This action is consistent with ICANN's mission and is in the public interest as it is important to ensure stability of ICANN organization in the way of a robust Reserve Fund in case use of a Reserve Fund becomes necessary. Furthermore, this action is consistent with ICANN's mission and is in the public interest as the SFICR will fund projects, as approved by the Board, when the size, complexity, and length of the projects create a challenge to be solely funded by recurring funding.

This action will not have a financial impact on ICANN, and will not have an impact on the security, stability, or resiliency of the domain name system.

This is an Organizational Administrative function that does not require public comment.

Submitted by:	Xavier Calvez
Position:	SVP, Planning and CFO
Date Noted:	28 June 2021
Email:	xaver.calvez@icann.org

ICANN BOARD SUBMISSION No. 2021.07.22.1d

TITLE: **Operating Fund Investment Policy Update**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

The Board is being asked to approve an update to the ICANN Investment Policy to allow for increased investment of funds in the Operating Fund and Supplemental Fund for Implementation of Community Recommendations (SFICR) into long-term, moderately liquid assets.

The update to the Investment Policy is prudent to ensure that ICANN org properly monetizes funds to outpace inflation while maintaining a low level of risk. (See redline of Investment Policy as Attachment A to the Reference Materials for this Board paper.)

The balance of the Operating Fund at the end of FY21 shows an excess of US$38,000,000 over the minimum of three months of operating expenses. ICANN organization has recommended that US$5,000,000 be transferred into the Reserve Fund and that US$15,000,000 be transferred to the SFICR. The remaining US$18,000,000 will be invested into long-term, moderate-yield instruments subject to the Board's approval of the revised ICANN Investment Policy.

ICANN ORGANZATION AND BOARD FINANCE COMMITTEE (BFC) RECOMMENDATIONS *(Subject to BFC Approval)*:

Both ICANN organization and the BFC recommend that the Board approve the proposed revisions to the ICANN Investment Policy.

PROPOSED RESOLUTION:

Whereas, the Operating Fund includes the funds used for ICANN's day-to-day operations and must contain enough funds to cover a minimum of three months of ICANN organization's operating expenses.

Whereas, the Supplemental Fund for Implementation of Community Recommendations (SFICR) allows ICANN to segregate resources in support of increasing the capacity of the organization to address projects that are multi-year and focus on community recommendations that are approved or soon to be adopted by the Board but do not fit within the annual budget.

Whereas, both ICANN organization and the Board Finance Committee have recommended that the Board approve an update to the ICANN Investment Policy to allow funds in the Operating Fund and SFICR to be invested in long-term investment instruments with moderate returns and a moderate liquidity level in order to outpace inflation while maintaining a low level of risk.

Resolved (2021-07-22-xx), the Board approves the revised ICANN Investment Policy that, as revised, allows funds in the Operating Fund and SFICR to be invested in long-term, moderate-yield, and moderately liquid investment instruments.

PROPOSED RATIONALE:

As part of ICANN's Investment Policy, the Operating Fund should be at a level of funds to cover a minimum of three months of ICANN organization's operating expenses, and that any amount determined to be in excess may be transferred to either the Reserve Fund, to ensure its balance is at or above the minimum target level, or the SFICR to increase the capacity of the organization to address projects that are multi-year and focus on community recommendations that are approved or soon to be adopted by the Board but cannot fit within the annual budget. In order to outpace inflation while maintaining a low level of risk, ICANN organization and the Board Finance Committee (BFC) recommended that funds in the Operating Fund and SFICR be invested in long-term investment instruments with moderate returns and a moderate liquidity level.

ICANN org and the BFC recommended this change because funds in the Operating Fund and SFICR are currently not being invested as their eligible investments would not yield worthwhile return. Hence, these funds are not keeping up with inflation and are therefore losing value. The ICANN Investment Policy revisions would allow investments in long-term and moderately liquid instruments, enabling ICANN org to achieve some return and outpace inflation while maintaining a low level of risk due to the nature of the instruments.

Adopting the suggested modifications to the ICANN Investment Policy is in the best interest of ICANN and its community because it will expand the available investment options to optimize potential returns within acceptable risk parameters, which is also consistent with ICANN's mission.

This action is very likely to have a positive financial impact on ICANN in that the additional investment options should yield higher earnings. This action will not have an impact on the security, stability, or resiliency of the domain name system.

This is an Organizational Administrative function that does not require public comment.

Submitted by:	Xavier Calvez
Position:	SVP Planning and CFO
Date Noted:	28 June 2021
Email:	xaver.calvez@icann.org

ICANN BOARD SUBMISSION No. 2021.07.22.1e

TITLE: **Los Angeles Office Lease Renewal**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

The Board is being asked to approve a new lease for ICANN's Los Angeles headquarters office lease. The new lease will be 10 years in duration, beginning July 2022 and ending June 2032.

ICANN's Headquarters office has been located in Playa Vista, California since 2012, and consists of approximately 50,000 square feet. The current lease is set to expire in June 2022.

ICANN org has evaluated the decision to renew or move, including evaluating properties with the help of its broker, in the context of the organization's expected workload over the next few years, and the impact of this workload on its workforce and operations. In this context, ICANN organization recommends staying at the existing location with no initial change to the square footage leased. The proposal is for a 10-year lease with average monthly costs of Confidential Negotiation Information . The increase in cost is reasonable given the real estate market in Los Angeles and alternative options, and ICANN org will be able to absorb the increase.

ICANN ORGANZATION AND BOARD FINANCE COMMITTEE (BFC) RECOMMENDATIONS*:*

ICANN organization recommends that the Board authorize the President and CEO, or his designee(s), to take all necessary actions to execute a new lease, and to make all necessary disbursements pursuant to the lease. The Board Finance Committee has reviewed the financial implications of the recommended lease renewal and concurs with ICANN org's recommendation.

PROPOSED RESOLUTION:

Whereas, ICANN's Los Angeles office lease is expiring in June 2022 and ICANN org recommends remaining at the current office location and entering into a new 10-year lease.

Whereas, the Board Finance Committee has reviewed the financial implications of the lease.

Whereas, both ICANN organization and the Board Finance Committee have recommended that the Board authorize the President and CEO, or his designee(s), to take all actions necessary to execute a new 10-year lease for ICANN's current Los Angeles office location, and to make all necessary disbursements pursuant to the lease.

Resolved (2021.07.22.xx) the Board authorizes the President and CEO, or his designee(s), to take all necessary actions to execute a new 10-year lease for ICANN's current Los Angeles office location, and to make all necessary disbursements pursuant to the lease.

Resolved (2021.07.22.xx), specific items within this resolution shall remain confidential for negotiation purposes pursuant to Article 3, section 3.5(b) of the ICANN Bylaws until the President and CEO determines that the confidential information may be released.

PROPOSED RATIONALE:

ICANN organization believes face to face interaction, including that which occurs at its headquarters, is essential to carry out its work and mission. Although the organization has been effectively operating remotely during the pandemic, the goal is to return to offices to support staff, and eventually community, collaboration at ICANN's physical office locations.

In 2012, ICANN signed a 10-year lease for 30,300 square feet of office space on the third floor of a Class A building in Playa Vista, California. ICANN added 5,782 square feet the following year and added 12,819 square feet in 2016 on the fourth floor of the building, along with tenant improvement customizations such as an interior staircase to connect the third and fourth floors, and a common area corridor on the fourth floor. ICANN now rents about 50,000 square feet total and its lease is set to expire in June 2022.

In early 2020, ICANN org began evaluating office space options upon the expiration of the current least. While evaluating properties, ICANN org considered the following criteria:

- Buildings of similar type and location to the current office

- ICANN's space requirements, including conference rooms
- Cost effectiveness
- Disruption to staff
- Amenities in the area
- Proximity to LAX and public transportation
- Safety and security
- If ICANN decided to move, the restoration cost to remove the interior staircase and restore the common area corridor on the fourth floor (about US$250,000)

After thorough consideration of many options, ICANN org began negotiating lease terms with the current landlord. The real estate market for suitable office space locations, such as the current space in Playa Vista, did not drop as much as other areas across the United States as a result of the pandemic. Given the current outlook of the pandemic and much of California reopening, market activity and rental rates have been steadily increasing. Because negotiations started during the pandemic, ICANN org is in a favorable bargaining position with the current landlord.

Confidential Negotiation Information

Early 2021, ICANN org evaluated all the parameters affecting the decision to stay at the current Play Vista headquarters or move to another location. The evaluation included consideration of the real estate market conditions set forth above, as well as the current and expected workload the organization is expecting to face, including multiple large, complex and new projects and activities that are expected to have a significant impact on the organization overall and on reshaping several teams specifically.

Although ICANN may save some money in the long term with some of these alternative options, in the context of workload, ICANN org has recommended staying at the current location to avoid disruption to staff and operations as well as the risks and costs of moving. Staying at the current location maintains the current building's safety and security, its ability to host board and community meetings, in addition to its proximity to airports, hotels, amenities, public transportation, and freeways.

Given the current market conditions and alternative property options, ICANN org recommended staying at the existing location and entering into a new 10-year lease. The Board Finance Committee has reviewed the financial implications of the lease and agrees with ICANN org's recommendation.

Executing the new office lease is in the public interest as it maintains ICANN's presence in Los Angeles where about half of ICANN org's staff is based. ICANN org will be able to continue to carry out ICANN's mission without disruption while maintaining collaboration with community stakeholders and the general public.

There will be a fiscal impact in average costs per month compared to the final year of the current lease. However, this increase is reasonable given the current real estate market and ICANN will be able to absorb the cost increase.

Taking this decision will have no anticipated impact to the security, stability, and resiliency of the domain name system.

This is an Organizational Administrative function that does not require public comment.

Submitted by:	Xavier Calvez
Position:	SVP, Planning and CFO
Date Noted:	25 June 2021
Email:	xaver.calvez@icann.org

ICANN BOARD PAPER NO. 2021.07.22.1f

TITLE: Board Committee Charter Amendments

PROPOSED ACTION: For Board Consideration and Approval

EXECUTIVE SUMMARY:

As part of its responsibilities, the Board Governance Committee (BGC) is tasked with "periodically review[ing] the charters of the Board Committees, including its own charter and work with the members of the Board Committees to develop recommendations to the Board for any charter adjustments deemed advisable." (BGC Charter, Sec. II.C.3.)

The BGC recommends that the Board review and adopt the revised charters for the BGC and the Board Risk Committee (BRC), attached to the Reference Materials as Attachments A and B, respectively. The proposed revisions to various sections of the BGC and BRC charters are relevant to bring the sections up to date with current practices and, as it relates to the BRC charter, it now includes reference to oversight of Risk Appetite Statement.

BOARD GOVERNANCE COMMITTEE RECOMMENDATIONS:

The BGC recommends that the Board approve amendments to the Board Governance Committee charter (attached as Attachment A to the Reference Materials) and the Board Risk Committee charter (attached as Attachment B to the Reference Materials).

PROPOSED RESOLUTION:

Whereas, the Board Governance Committee (BGC) is tasked with "periodically review[ing] the charters of the Board Committees, including its own charter and work with the members of the Board Committees to develop recommendations to the Board for any charter adjustments deemed advisable." (BGC Charter, § II.C.2.)

Whereas, the BGC has recommended that the Board approve revisions to various sections of the BGC and Board Risk Committee (Brc) charters.

Resolved (2021.07.22.XX), the Board hereby adopts the revised Board Governance Committee Charter.

Resolved (2021.07.22.XX), the Board hereby adopts the revised Board Risk Committee Charter.

PROPOSED RATIONALE:

The Board is addressing this matter to ensure committee charters are up-to-date and reflect the most current governance requirements and best practices.

As part of its responsibilities, the BGC is tasked with "periodically review[ing] the charters of the Board Committees, including its own charter and work with the members of the Board Committees to develop recommendations to the Board for any charter adjustments deemed advisable." (BGC Charter, Sec. II.C.3.) In this role, the BGC recommended, and the Board agrees, that Board approve revisions to the BGC anf BRC Committee charters to update the relevant sections of the charters to current practices. And, as it relates to the BRC charter, it now includes reference to oversight of Risk Appetite Statement.

This action is consistent with ICANN's Mission and is in the public interest as it is important to ensure that the Board has the necessary Committees, properly tasked with responsibilities, to ensure oversight over the ICANN organization, as the Board deems appropriate.

There will be no direct fiscal impact or adverse ramifications on ICANN's strategic and operating plans from the proposed changes to the charters.

There are no security, stability or resiliency issues relating to the domain nane system as the result of this action.

This decision is an Organizational Administrative Function that does not require public comment.

Submitted By:	Amy A. Stathos
Date:	23 October 2021
Email:	amy.stathos@icann.org

Board Governance Committee Charter | As approved by the ICANN Board of Directors on XX Xxxx XXXX

I. Purpose

The Board Governance Committee is responsible for:

A. Assisting the Board to enhance its performance;

B. Leading the Board in periodic review of its performance, including its relationship with ICANN's Chief Executive Officer;

C. Creating and recommending to the full Board for approval a slate of nominees for Board Chair, Board Vice Chair, Chair and membership of each Board Committee, including filling any vacancies which may occur in these positions during the year; and overseeing the creation and membership of Board Working Groups and Board Caucuses;

D. Oversight of compliance with ICANN's Board of Directors' Code of Conduct;

E. Administration of ICANN's Conflicts of Interest Policy;

F. Recommending to the Board corporate governance guidelines applicable to ICANN as a global, private sector corporation serving in the public interest;

G. Recommending to the Board a nominee for the Chair of the Nominating Committee and a nominee for the Chair-Elect of the Nominating Committee; and

H. Coordinating the dynamic development of the Board priorities and their associated deliverables, and monitoring progress against the set priorities.

II. Scope of Responsibilities

A. Assisting the Board to enhance its performance.

1. The Committee will serve as a resource for Directors in developing their

full and common understanding of their roles and responsibilities as Directors as well as the roles and responsibilities of ICANN. The Committee will provide guidance and assistance in orienting new Directors as the Board's membership evolves. It will help reinforce the Board's commitment to adhere to its Bylaws and Core Values.

2. The Committee will encourage the development of effective tools, strategies, and styles for the Board's discussions. The Committee will periodically review tools, templates, and guidelines for Board preparatory materials and reports.

3. The Committee will work closely with the Chair and Vice-Chair of the Board and the President and Chief Executive Officer (CEO) of ICANN.

B. Leading the Board in its periodic review of its performance, including its relationship with the ICANN President and CEO.

1. The Committee will develop a thoughtful process for the Board's self-analysis and evaluation of its own performance and undertake this process at least every two years. The Committee will consider, as appropriate, any external input that speaks directly to the performance of the Board.

2. The Committee will develop a sound basis of common understanding of the appropriate relationship between the Board and the President and CEO under the Bylaws. From time to time it will review and advise on the effectiveness of that important relationship.

3. The Committee will serve as a resource to Directors and the Chief Executive Officer by stimulating the examination and discussion of facts and analysis to complement anecdotal and other information acquired by individual directors from members of the community. In this way the Committee will assist the Board to distinguish among systemic problems, chronic problems, and isolated problems and will focus the Board's attention to both facts and perceptions.

C. Creating and recommending to the full Board for approval a slate of nominees for Board Chair, Board Vice Chair, Chair and membership of each Board Committee, including filling any vacancies which may occur in these positions during the year; and overseeing the creation and membership of Board Working Groups and Board Caucuses.

1. In accordance with the Board Governance Committee Procedures for Board Nominations posted on the Committee webpage, the Committee will: (a) in advance of the Annual General Meeting (AGM) create for Board approval a new slate of nominees to serve on each committee for the upcoming year; (b) fill any vacancies that arise during the year; and (c) recommended to the Board committee appointments for Board members beginning their terms on a date other than at AGM.

2. The Committee shall oversee the creation and membership of Board working groups and Board caucuses.

3. The Committee shall periodically review the charters of the Board Committees, including its own charter and work with the members of the Board Committees to develop recommendations to the Board for any charter adjustments deemed advisable.

4. The Committee may serve as a resource for the Chief Executive Officer and Directors who are considering the establishment of new committees.

5. The Committee shall periodically review the participation of Board members across Board Committees, working groups, and/or caucuses, and make recommendations to the Board of adjustments to the composition of any Board Committees, Working Groups and/or Caucuses, as necessary to ensure that 1) the workload of Board members is appropriately balanced across the Board and 2) the Board Committees, Working Groups and/or Caucuses have the right mix of skills and expertise among Board members to accomplish their respective goals.

D. Oversight of compliance with ICANN's Board of Directors' Code of Conduct.

1. The Committee shall be responsible for oversight and enforcement with respect to the Board of Directors' Code of Conduct. In addition, at least annually, the Committee will review the Code of Conduct and make any recommendations for changes to the Code to the Board.

2. The Committee shall provide an annual report to the full Board with respect to compliance with the Code of Conduct, including any breaches and corrective action taken by the Committee.

E. Administration of ICANN's Conflicts of Interest Policy.

1. The Committee shall review the annual conflicts of interest forms required from each Directors and Liaisons and shall consider any and all conflicts of interest that may arise under the Conflicts of Interest Policy.

2. The Committee shall periodically review the Conflicts of Interest Policy and consider whether any modifications should be made to the policy to improve its effectiveness**.**

F. Recommending to the Board corporate governance guidelines applicable to the ICANN as a global, private sector corporation serving in the public interest.

1. The Committee shall review, at least every four years but in line with best practices, the existing corporate governance guidelines developed by ICANN staff, be attentive to developments in corporate governance in the global context, and bring ideas and recommendations for adjustments in these guidelines to the Board for its consideration.

G. Recommending to the Board a nominee for the Chair of the Nominating Committee and a nominee for the Chair-Elect of the Nominating Committee.

1. Annually the Committee shall identify, through informal and formal means, and recommend that the Board approve a nominee to serve as Chair of the Nominating Committee and a nominee to serve as the Chair-Elect of the Nominating Committee.

H. Coordinating the dynamic development of the Board priorities and their associated deliverables, and monitoring progress against the set priorities.

III. Composition

The Committee shall be comprised of at least three but not more than seven Board members, as determined and appointed annually by the Board, each of whom shall comply with the Conflicts of Interest Policy. The voting Directors on

the Committee shall be the voting members of the Committee, and the majority of the Committee members must be voting Directors. The members of the Committee shall serve at the discretion of the Board.

Unless a Committee Chair is appointed by the full Board, the members of the Committee may designate its Chair from among the voting members of the Committee by majority vote of the full Committee membership.

The Committee may choose to organize itself into subcommittees to facilitate the accomplishment of its work. The Committee may seek approval and budget from the Board for the appointment of consultants and advisers to assist in its work as deemed necessary, and such appointees may attend the relevant parts of the Committee meetings.

IV. Meetings

A. Regularly Scheduled Meetings

The Board Governance Committee shall meet at least quarterly, or more frequently as it deems necessary to carry out its responsibilities. The Committee's meetings may be held by telephone and/or other remote meeting technologies. Meetings may be called upon no less than forty- eight (48) hours notice by either (i) the Chair of the Committee or (ii) any two members of the Committee acting together, provided that regularly scheduled meetings generally shall be noticed at least one week in advance.

B. Special/Extraordinary Meetings

Special/extraordinary meetings may be called upon no less than 48 hours notice by either (i) the Chair of the Committee or (ii) any two members of the Committee acting together. The purpose of the meeting must be included with the call for the meeting.

C. Action Without a Meeting

i. Making a Motion:

The Committee may take an action without a meeting for an individual

item by using electronic means such as email. An action without a meeting shall only be taken if a motion is proposed by a member of the Committee, and seconded by another voting member of the Committee. All voting members of the Committee

must vote electronically and in favor of the motion for it to be considered approved. The members proposing and seconding the motion will be assumed to have voted in the affirmative. The action without a meeting and its results will be noted in the next regularly scheduled Committee meeting and will be included in the minutes of that meeting.

ii. Timing:

a. Any motion for an action without a meeting must be seconded by another Committee member within 48 hours of its proposal.

b. The period of voting on any motion for an action without a meeting will be seven (7) days unless the Chair changes that time period. However, the period must be a minimum of two (2) days and a maximum of seven (7) days.

V. Voting and Quorum

A majority of the voting members of the Committee shall constitute a quorum. Voting on Committee matters shall be on a one vote per member basis. When a quorum is present, the vote of a majority of the voting Committee members present shall constitute the action or decision of the Committee.

VI. Records of Proceedings

A preliminary report with respect to actions taken at each meeting (telephonic or in-person) of the Committee shall be recorded and distributed to committee members within two working days, and meeting minutes shall be posted promptly following approval by the Committee.

A report of the activities of the Committee shall be prepared and published semiannually.

VII. Succession Plan

The Board Governance Committee shall maintain a succession plan for the Committee, which should include identifying the experience, competencies and personal characteristics required to meet the leadership needs of the Committee. The Committee shall annually review the succession plan to ensure that it meets the needs of the Committee.

VIII. Review

The Board Governance Committee shall conduct a self-evaluation of its performance on an annual basis and share a report on such self-evaluation with the full Board and shall recommend to the full Board changes in membership, procedures, or responsibilities and authorities of the Committee if and when deemed appropriate. Performance of the Board Governance Committee shall also be formally reviewed as part of the periodic independent review of the Board and its Committees.

Risk Committee Charter | As approved by the ICANN Board of Directors on XX Xxx XXXX

1. Purpose

The Risk Committee of the ICANN Board is responsible for the assessment and oversight of policies implemented by ICANN designed to manage ICANN's risk profile, including the establishment and implementation of standards, controls, limits and guidelines related to risk assessment and risk management, including but not limited to financial, technical, legal and operational risks and other risks concerning ICANN's reputation and ethical standards.

2. Scope of Responsibilities

The following responsibilities are set forth as a guide for fulfilling the Committee's purposes. The Committee is authorized to carry out these activities and other actions reasonably related to the Committee's purposes as may be assigned by the Board from time to time:

1. Oversight of risk management for ICANN as an organization, including the following activities:
    1. Reviewing and advising on the ICANN risk management framework and associated policies, plans, programs, and reporting relating to risk management;
    2. Monitoring the effectiveness of the risk management framework;
    3. Oversight of the significant non-financial risk exposure for ICANN and steps taken to monitor and control such exposure;
    4. Staying informed on conditions at ICANN in order to identify potential future risks and advise on plans for addressing these risks as appropriate;
    5. Reviewing other areas of risk concentration as appropriate, including coordinating with other committees of the Board which review risk, as well risks identified arising from the work of the ICANN community; and
    6. Reviewing and providing oversight to the Risk Appetite Statement, and assessing the alignment and compliance of the

Deleted: 2

Deleted: November 2017

Deleted: Process and Systems

Deleted: and

Deleted: programs, including operational risk management and controls

Deleted: conditions and gaining familiarity with ICANN processes

Deleted: and

Deleted: .

Formatted: Right: 0.25"

Statement with the org Risk Register and the ICANN Strategic Plan.

2. Oversight of operational activities relating to risk management including reviewing information and monitoring the effectiveness of risk management activities such as:

    1. The effectiveness of the technology utilized by ICANN focusing on Info and Cyber Security;

    2. The adequacy of ICANN's business continuity policies; and

    3. Addressing changes in the Internet ecosystem (technology, business environment, community, etc.) that may be material to ICANN operations.

3. Informing and advising the Board on the outcomes of these oversight areas, the Committee recommendations and assessment of those outcomes, if any, as well as other reporting deemed appropriate by the Committee.

3. Composition

The Committee shall be comprised of at least three but not more than seven Board members, as determined and appointed annually by the Board, each of whom shall comply with the Conflicts of Interest Policy. The voting Directors on the Committee shall be the voting members of the Committee, and the majorit of the Committee members must be voting Directors. The members of the Committee shall serve at the discretion of the Board.

The Committee shall have a Chair and may have a co-Chair or vice-Chair. Unless a Committee Chair/co-Chair/vice-Chair is appointed by the full Board, the members of the Committee may designate its Chair/co-Chair/vice-Chair from among the members of the Committee by majority vote of the full Committee membership.

The Committee may choose to organize itself into subcommittees to facilitate the accomplishment of its work. The Committee may seek approval and budget from the Board for the appointment of consultants and advisers to assist in its work as deemed necessary, and such appointees may attend the relevant parts of the Committee meetings.

4. Meetings

1. Regularly Scheduled Meetings.

    The Committee shall meet at least three times per year, or more frequently as it deems necessary to carry out its responsibilities. The schedule of these meetings will be established at the beginning of the calendar year. The

Deleted: of the

Deleted: of operational

Deleted: business environment

Formatted: Right: 0.25"

Committee's meetings may be held by telephone and/or other remote meeting technologies. Regularly scheduled meetings shall be noticed at least one week in advance, unless impracticable, in which case the notice shall be as soon as practicable.

2. Special/Extraordinary Meetings.

   Special/Extraordinary meetings may be called upon no less than forty-eight (48) hours notice by either (i) the Chair of the Committee or (ii) any two members of the Committee acting together. The purpose of the meeting must be included with the call for the meeting.

3. Action Without a Meeting
    1. Making a Motion:

       The Committee may take an action without a meeting for an individual item by using electronic means such as email. An action without a meeting shall only be taken if a motion is proposed by a member of the Committee, and seconded by another voting member of the Committee. All voting members of the Committee must vote electronically and in favor of the motion for it to be considered approved. The members proposing and seconding the motion will be assumed to have voted in the affirmative. The action without a meeting and its results will be noted in the next regularly scheduled Committee meeting and will be included in the minutes of that meeting.

    2. Timing:
        1. Any motion for an action without a meeting must be seconded by another Committee member within 48 hours of its proposal.

        2. The period of voting on any motion for an action without a meeting will be seven days unless the Chair changes that time period. However, the period must be a minimum of two days and a maximum of seven days.

5. Voting and Quorum

A majority of the voting members shall constitute a quorum. Voting on Committee matters shall be on a one vote per member basis. When a quorum is present, the vote of a majority of the voting Committee members present shall constitute the action or decision of the Committee.

6. Recording of Proceedings

Formatted: Right: 0.25"

A preliminary report with respect to actions taken at each meeting (telephonic or in-person) of the Committee shall be recorded and distributed to committee members within two working days, and meeting minutes shall be posted promptly following approval by the Committee.

An report of the activities of the Committee shall be prepared and published semiannually.

7. Succession Plan

The Board Risk Committee shall maintain a succession plan for the Committee which includes identifying competencies and personal characteristics required to meet the leadership needs of the Committee. The Committee shall annually review the succession plan to ensure that it meets the needs of the Committee.

8. Review

The performance of the Committee shall be reviewed annually and informally by the Board Governance Committee. The Board Governance Committee shall recommend to the full Board changes in membership, procedures, or responsibilities and authorities of the Committee if and when deemed appropriate. Performance of the Committee shall also be formally reviewed as part of the periodic independent review of the Board and its Committees.

Formatted: Right: 0.25"

REFERENCE MATERIALS – BOARD SUBMISSION NO. 2021.02.XX.XX

TITLE: Board Committee Charter Amendments

Documents

The following attachment is relevant to the Board's consideration of the proposed revisions to the charters of the Board Governance Committee and Board Risk Committee.

Attachment A is the proposed revised Charter of the Board Governance Committee in redlined format.

Attachment B is the proposed revised Charter of the Board Risk Committee in redlined format.

Submitted By:	Amy Stathos, Deputy General Counsel
Date Noted:	21 July 2021
Email:	amy.stathos@icann.org

ICANN BOARD PAPER NO. [To be assigned by the Secretary]

TITLE: Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

PROPOSED ACTION: For Board resolution

EXECUTIVE SUMMARY:

The Board is being asked to take action on the recommendations of the community-led second Security, Stability, and Resiliency (SSR2) Review Team. In accordance with Section 4.6 of the ICANN Bylaws, the final report issued by the SSR2 Review Team assesses "ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates."

The Security, Stability, and Resiliency (SSR) Review is one of four Specific Reviews anchored in the ICANN Bylaws and relates to key elements of the ICANN's Strategic Plan. Section 4.6 of the ICANN Bylaws requires the Board to take action on the SSR2 Review Team Final Report within six months of receipt, by 25 July 2021.

The SSR2 Review Team issued 63 recommendations in its final report; many recommendations are complex and touch on other significant areas of work underway and therefore cannot be addressed in silos. The Board's consideration of the ICANN organization's (ICANN org) detailed assessment takes into account interdependencies with other ongoing efforts within the community and ICANN org, initial reflections on resources, and the public comment submissions received. The Board notes that it will be important for implementation of any recommendations to complement existing advice, other community recommendations, public input, and also align with ICANN's Strategic Plan.

Noting some broad areas and themes in relation to the SSR2 recommendations, many of which are emphasized in public comments, the Board developed six categories of Board action on

SSR2 recommendations to move some recommendations to final action now, while allowing for sufficient additional time for fulsome analysis and consideration of the relevant significant factors impacting the feasibility of implementing other recommendations. The categories include:

- Recommendations the Board approves, subject to prioritization, risk assessment and mitigation, costing and implementation considerations; and recommendations that the Board approves, with the understanding that they are already fully implemented. Approved recommendations are consistent with ICANN's Mission, serve the public interest, and fall within the Board's remit. Further, approved recommendations are clear, do not have dependencies (including any requiring mitigation of other work), have community support and a clear path to implementation.
- Recommendations the Board rejects because the recommendation cannot be approved in full. The Board notes that, while some portions of the recommendation could be feasible, and in some cases, work is already underway, there are limitations imposed by other portions of the same recommendation that could impact feasibility. While the Board agrees in principle with the intent of many of these recommendations, the Board does not have the option of selectively approving some parts and rejecting other parts of a single, indivisible community recommendation and must act on a recommendation as written and not as interpreted by ICANN org or the Board. The detailed rationale for each recommendation sets out the specific reasons for the Board's rejection.
- Recommendations the Board rejects. The detailed rationale for each recommendation sets out the specific reasons for the Board's rejection.
- Recommendations that the Board determines to be pending, likely to be approved once further information is gathered to enable approval. The Board expects specific actions to take place in order to take further Board decision on these recommendations. The Board uses this category to communicate to the ICANN community that, based on the information available to date, the Board anticipates that each of these recommendations will be approved.

- Recommendations that the Board determines to be pending, holding to seek clarity or further information. The Board is unable to signal at this time whether it is likely to accept or reject each of these recommendations pending the collection of additional information.
- Recommendations that the Board determines to be pending, likely to be rejected unless additional information shows implementation is feasible. The Board expects specific actions to take place in order to take further Board decision on these recommendations. The Board uses this category to communicate to the ICANN community that, based on the information available to date, the Board anticipates that each of these recommendations will be rejected.

This categorization allows for community communications and transparency on how ICANN org and Board assessed and considered the recommendations, while ensuring Board accountability to the Bylaws-mandated deadline to take action on the recommendations within six months of receipt of a final report. The Bylaws require that for every Specific Review recommendation that the Board does not accept, the Board must provide a rationale supporting its action, and a draft rationale is provided for the Board's consideration.

Approved recommendations will be subject to prioritization, risk assessment and mitigation, costing and implementation considerations as noted in the Board action for each recommendation. Some recommendations proposed for Board approval call for actions that have already been implemented by ICANN org. Based on the supplied evidence of implementation, there will be no further action required from ICANN org and the implementation of these recommendations will be considered complete. For recommendations that the Board will place into the pending categories, the Board commits to take further action on these recommendations subsequent to the completion of intermediate steps as identified in the Scorecard. Within six months of this Board action, ICANN org will provide the Board with the information as requested in the Scorecard, and will advise the Board if additional time is needed to support the Board in reaching a decision on the pending recommendations.

ORGANIZATIONAL EFFECTIVENESS COMMITTEE RECOMMENDATION:

The Organizational Effectiveness Committee of the ICANN Board (OEC) is responsible for the oversight of all Specific Reviews mandated by Section 4.6 of the ICANN Bylaws, including the Security, Stability, and Resiliency review. The OEC recommends that the Board take action on the recommendations in the SSR2 Review Team Final Report, as enumerated in the Scorecard titled "Final SSR2 Review Team Recommendations - Board Action." The OEC makes its recommendation to the Board based on inputs from the Board Caucus on SSR2, and based on its determination that the process was in compliance with the relevant Bylaw provisions, in accordance with the Board-adopted Operating Standards for Specific Reviews.

PROPOSED RESOLUTION:

Whereas, under Section 4.6 of the ICANN Bylaws, ICANN is obligated to conduct a "periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates ('SSR Review')." A community-led review team - the second Security, Stability, and Resiliency (SSR2) Review Team - was announced on 14 February 2017 to fulfill that mandate.

Whereas, on 28 October 2017, the ICANN Board, in consideration of concerns received, sent a letter to the SSR2 Review Team to suspend its work, pending input from ICANN Supporting Organizations (SOs) and Advisory Committees (ACs) on any need to adjust the scope, terms of reference, work plan, skill set and/or resources allocated to the SSR2 Review.

Whereas, the suspension generated a dialog between SO/ACs chairs and ICANN Board and led to a request for additional membership on the SSR2 Review Team and the engagement of an external facilitator to assist the review team in resolving issues of scope, membership, and other

concerns as raised. On 7 June 2018, ICANN org announced the formal restart of the SSR2 Review Team.

Whereas, on 24 January 2020, the SSR2 Review Team released a draft report for public comment.

Whereas, on 25 January 2021, the SSR2 Review Team submitted a final report containing 63 full consensus recommendations to the ICANN Board for consideration.

Whereas, the SSR2 Review Team Final Report is the culmination of nearly four years of work by 17 review team members, representing over 2,800 hours of meetings and countless more hours of work.[1]

Whereas, the SSR2 Review Team Final Report was published for public comment on 28 January 2021 to inform Board action on the report, in accordance with Bylaw requirements. The summary of community input received on the final report highlights a variety of viewpoints, including community views on which recommendations the Board should act on quickly as well as which recommendations the Board should consider rejecting.

Whereas, the Board has devoted significant time to following the SSR2 Review Team's work, including through the Organizational Effectiveness of the ICANN Board (OEC) and the Board Caucus Group on SSR2 (SSR2 Caucus), to achieve this decision today.

Whereas, on 20 July 2021, the OEC discussed and approved its recommendation that the Board take action on the recommendations in the SSR2 Review Team Final Report, as enumerated in the Scorecard titled "Final SSR2 Review Team Recommendations - Board Action." The OEC's recommendation was informed by the work of the SSR2 Caucus, which was established and included the Board-appointed members of the SSR2 Review Team. The SSR2 Caucus led the Board's efforts in reviewing the recommendations and ICANN org's assessments and supports the substantive action on the recommendations as provided to the Board.

[1] Based on the SSR2 Fact Sheet dated 31 March 2021: https://community.icann.org/x/S7zRAw

Resolved (2021.07.22.xx), the Board thanks the members of the SSR2 Review Team for their dedication and work to achieve the SSR2 Review Team Final Report.

Resolved (2021.07.22.xx), the Board takes action on each of the 63 recommendations issued within the SSR2 Review Team Final Report, as specified within the Scorecard titled "Final SSR2 Review Team Recommendations - Board Action." The Board directs ICANN's President and CEO, or his designee(s), to take all actions as directed within that Scorecard.

Resolved (2021.07.22.xx), for the 34 recommendations placed into one of the three pending statuses, the Board commits to take further action on these recommendations subsequent to the completion of steps as identified in the Scorecard. The Board directs the ICANN President and CEO, or his designee(s), to provide to the Board relevant information, as requested in the Scorecard, or periodic updates on progress toward gathering relevant information, starting within six months from this Board action, in order to support further Board action on each recommendation.

PROPOSED RATIONALE:

Why is the Board addressing the issue?

The Security, Stability, and Resiliency (SSR) Review is one of the four Specific Reviews anchored in Section 4.6 of the ICANN Bylaws. Specific Reviews are conducted by community-led review teams, which assess ICANN's performance in fulfilling its commitments. Reviews are critical to maintaining an effective multistakeholder model and helping ICANN achieve its Mission, as detailed in Article 1 of the Bylaws. Reviews also contribute to ensuring that ICANN serves the public interest. The SSR2 Review is the second iteration of the SSR Review and relates to key elements of ICANN's Strategic Plan.

SSR2 recommendations are considerable in number (63 recommendations) and many are complex and touch on other significant areas of work underway - for example, DNS security threats/DNS abuse, New Generic Top-Level Domain (gTLD) Subsequent Procedures, and Name

Collision. Given the strategic significance of security, stability, and resiliency of the DNS within the ICANN ecosystem, the Board notes that the recommendations from SSR2 Review Team cannot be considered in silos and require fulsome analysis and consideration.

What is the proposal being considered?

The Board today considers the 63 consensus recommendations within the SSR2 Review Team Final Report. Issues assessed by the SSR2 Review Team include: the extent to which prior SSR Review recommendations have been implemented and whether implementation has resulted in the intended effect; key stability issues within ICANN; contracts, compliance, and transparency around Domain Name System (DNS) security threats; and additional SSR-related concerns regarding the global DNS.

The Board reviewed public comments on the SSR2 Review Team Final Report and briefings by ICANN org on the feasibility and impact of implementation of recommendations, taking into account initial reflections on resources and interdependencies with other ongoing efforts within the community. In reviewing public comments, the Board notes that comments represent a significant diversity of views. In addition to making comments on the individual recommendations and/or recommendation groupings as defined by the SSR2 Review Team, most community groups also provided general or overarching comments about the report as a whole. The International Trademark Association (INTA), Business Constituency (BC), At-Large Advisory Committee (ALAC) and Intellectual Property Constituency (IPC) make statements of overall support for all of the recommendations contained in the SSR2 Review Team Final Report, in several cases highlighting recommendations of particular importance to their members that they encourage the Board to consider as high priority. Several commenters registered overarching concerns, as noted in the themes below, such as concerns that recommendations repeat, duplicate or significantly overlap with existing ICANN org operations, and concerns that recommendations contemplate that the Board or ICANN org should unilaterally develop policy outside of the Generic Names Supporting Organization (GNSO) Council's Policy Development Process.

Board Approach to Consideration

The Board sets out below some broad areas and themes that it took into consideration in relation to the SSR2 recommendations, many of which are emphasized in public comments. In light of these themes and considerations, the Board developed six categories of Board action on SSR2 recommendations to move some recommendations to final action now, while allowing for sufficient additional time for fulsome analysis and consideration of the relevant significant factors impacting the feasibility of implementing other recommendations. The categories are:

- Recommendations the Board approves, subject to prioritization, risk assessment and mitigation, costing and implementation considerations; and recommendations that the Board approves, with the understanding that they are already fully implemented. Approved recommendations are consistent with ICANN's Mission, serve the public interest, and fall within the Board's remit. Further, approved recommendations are clear, do not have dependencies (including any requiring mitigation of other work), have community support and a clear path to implementation.
- Recommendations the Board rejects because the recommendation cannot be approved in full. The Board notes that, while some portions of the recommendation could be feasible, and in some cases, work is already underway, there are limitations imposed by other portions of the same recommendation that could impact feasibility. While the Board agrees in principle with the intent of many of these recommendations, the Board does not have the option of selectively approving some parts and rejecting other parts of a single, indivisible community recommendation and must act on a recommendation as written and not as interpreted by ICANN org or the Board. The detailed rationale for each recommendation sets out the specific reasons for the Board's rejection.
- Recommendations the Board rejects. The detailed rationale for each recommendation sets out the specific reasons for the Board's rejection.
- Recommendations that the Board determines to be pending, likely to be approved once further information is gathered to enable approval. The Board expects specific actions to take place in order to take further Board decision on these recommendations. The Board

uses this category to communicate to the ICANN community that, based on the information available to date, the Board anticipates that each of these recommendations will be approved.

- Recommendations that the Board determines to be pending, holding to seek clarity or further information. The Board is unable to signal at this time whether it is likely to accept or reject each of these recommendations pending the collection of additional information.
- Recommendations that the Board determines to be pending, likely to be rejected unless additional information shows implementation is feasible. The Board expects specific actions to take place in order to take further Board decision on these recommendations. The Board uses this category to communicate to the ICANN community that, based on the information available to date, the Board anticipates that each of these recommendations will be rejected.

In assessing and considering the SSR2 recommendations, the Board reviewed various significant materials and documents, including the Report of Public Comments on the SSR2 Draft Report, the Report of Public Comments on the Final Report, and the ICANN org assessment of SSR2 recommendations. The Board engaged with the community and listened carefully to community discussions regarding the SSR2 recommendations during the ICANN70 Virtual Community Forum and the ICANN71 Virtual Policy Forum to better understand the complexities of the recommendations and their potential impacts. The Board, with the support of ICANN org, analyzed the 63 recommendations noting dependencies and considerations for each, including significant interdependencies of the SSR2 recommendations with other community work, recent advice and public input. As part of this analysis and in considering action on each of the recommendations, the Board and ICANN org factored in the measures of success as defined by the SSR2 Review Team in its final report. In the case of several recommendations, the Board notes that, as written, implementation can never be deemed successful or effective based on the measures of success as defined by the SSR2 Review Team, and as such, the Board requires confirmation

or clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent.

The categorization approach allows for additional community consultation and information gathering where necessary, such as where recommendations are not clear or present inconsistencies with advice or other community work and public input. Further, the approach ensures Board accountability to the Bylaws-mandated deadline to take action on the recommendations within six months of receipt of a final report. The Bylaws require that for every Specific Review recommendation that the Board does not accept, the Board must provide a rationale supporting its action.

Identified Themes and Considerations

The themes and considerations that guided the Board's decision-making include:

SSR2 recommendations are considerable in number, complex, and have interdependencies with other significant areas of work underway.

The SSR2 Review Team organized 63 distinct recommendations into 24 groups, with one single recommendation on the implementation of SSR1 recommendations comprising 28 underlying recommendations. The Board notes that 23 recommendations issued by the SSR2 Review Team relate to DNS security threats/DNS abuse, while others also relate to other significant areas of work underway within ICANN, such as New gTLD Subsequent Procedures and Name Collision.

Some recommendations contain components that the Board cannot approve, along with components that are feasible, and in some cases already being done.

The Board notes that there are some recommendations for which some portions appear feasible (or reflect work already being done), yet there are limitations imposed by the other portions of the same recommendation that could impact feasibility.

The Board notes that part of the community intent in incorporating Specific Reviews into the ICANN Bylaws in 2016 was to require the Board act on recommendations as written, not as interpreted by ICANN org or Board. The Board understands this limitation also prevents the Board from selectively approving some parts and rejecting other parts of a single, indivisible community recommendation. Though the Board is not able to selectively approve portions of recommendations, and as a result must reject some recommendations in their entirety, the Board still recognizes that it is important to acknowledge where work and further efforts could be achieved. Though the Board might direct ICANN org to take some actions on rejected recommendations, such actions will not be tracked as part of the tracking of the implementation of approved SSR2 recommendations.

Considering these factors, the Board placed several recommendations into a category "reject because the recommendation cannot be approved in full", even though the Board agrees in principle with the intent of the recommendation and identifies all efforts that it understood as supporting the broader intent of each recommendation.

Some recommendations are polarizing, with public comments reflecting different, often opposing views.

Recent advice and public input on SSR topics further suggest that the Board and org should ensure full analysis and consideration, and where needed, additional community consultation, of inconsistencies with advice or other community work and public input. Implementation of any recommendations should complement existing advice, Board-accepted recommendations, and public input, and should align with ICANN's role in security, stability, and resiliency.

Several recommendations repeat, duplicate or significantly overlap with existing ICANN org operations, or recommendations issued by other Specific Review teams

The gTLD Registries Stakeholder Group (RySG), Public Interest Registry (PIR), i2Coalition, Namecheap, and the Registrar Stakeholder Group (RrSG) express concerns that some recommendations repeat or significantly overlap with ongoing work, including ICANN org

work, cross-community work, policy processes such as the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team, and recommendations from other review teams including the Competition, Consumer Trust, and Consumer Choice (CCT) Review Team. For example:

- RySG - "We cannot support recommendations that repeat, or represent significant overlap with, recommendations of other active reviews such as the CCT-RT and policy processes such as the EPDP. The RySG questions the value in implementing repetitive recommendations and urges the Board to consider the impact on the workloads of the community and Staff, and to reject those where implementation would circumvent the policy development process or where similar past recommendations have not been accepted by the Board...we would like to urge the Board to consider the wealth of DNS Abuse work that is ongoing in the community and to not accept recommendations that would duplicate those efforts or risk to undo progress made in recent months."
- PIR - "We note that several recommendations represent significant duplication of ongoing cross community work and recommendations from the CCT RT, many of which focus on the issue of DNS Abuse."
- i2Coalition - "The i2Coalition is in support of the community work already happening throughout the whole of ICANN, and believes that recommendations which are repetitive or directly duplicative are not in the best interest of ICANN.... For instance, Recommendation 17 is potentially duplicative with the existing Name Collision Analysis Project (NCAP) study. There are certainly several others throughout the report that merit thorough exploration before any action is taken on them."
- RrSG - "A number of recommendations cover items that ICANN org is already dedicating significant resources- including the responsibilities of the Office of the Chief Technology Officer (OCTO) and Contractual Compliance."
- Namecheap - "A number of the recommendations in the SSR2 Final Report address items or functions that ICANN org already provides- and in some cases is already dedicating significant resources toward."

Noting the public input on recommendations that duplicate or significantly overlap with existing ICANN org operations or recommendations issued by other Specific Review teams, the Board is taking the action of placing many of these recommendations into a pending category, directing ICANN org to complete the intermediate steps that would support in eventually accepting or rejecting each recommendation. These intermediate steps include seeking clarification from the SSR2 Implementation Shepherds, consulting with the ICANN community or monitoring developments of activities that are dependencies.

Some recommendations contemplate that the ICANN Board or ICANN org should unilaterally develop policy outside of the GNSO Council's Policy Development Process.

Some commenters note concerns that some SSR2 recommendations as written do not respect the Bylaws-mandated policy development roles within the multistakeholder model. RySG, PIR, Tucows, Namecheap, and RrSG all note that they do not support recommendations that contemplate modifications to the Registry Agreement (RA) or the Registrar Accreditation Agreement (RAA) outside of the defined Policy Development Process (PDP) or contract negotiations process. For example:

- RySG - "Several recommendations suggest direct changes to the Registry Agreement. Changes to Registry Agreements may only be made through the policy development process or by triggering a formal negotiation and amendment process."
- PIR - "Several SSR2 recommendations would represent violations of the terms of the Registry Agreement which governs the inclusion of third-party interests in contractual negotiations and how temporary policies/specifications may be used by ICANN."
- Tucows - "The Tucows family of registrars notes the long-term efforts that the Registrars and Registries have undertaken with ICANN Org in order to attempt to negotiate new contractual clauses that other ICANN Community-led efforts have recommended including, but not limited to, the current renegotiation of the RAA and the ongoing discussions surrounding a data processing addendum to both the RAA and the RA. The existence and nature of these negotiations clearly indicates that ICANN Org and the

Contracted Party House continue to work together to make necessary contractual amendments and that no other party should be involved in that process."

- Namecheap - "Namecheap does not support any of the components of the SSR2 Final Report that contemplate any modification of the RAA (including but not limited to Recommendations 6 and 8), and urges the ICANN Board to completely reject any of these recommendations. Namecheap is concerned that the recommendations in the SSR2 Final Report appear to be a method of subverting the ICANN multistakeholder model- rather than focusing on ICANN's status and progress in the security and stability of the Internet's unique identifiers (as Specified in Section 4.6(c) of the ICANN Bylaws)."
- RrSG - "A number of the recommendations include specific instructions to ICANN to change the RAA and the RA. The RrSG notes that these recommendations are contrary to the negotiation process identified in the RAA (Section 7.4), and the RA (Article 7.7), and should be completely rejected by the ICANN Board."

The Board and ICANN org take in the inputs of the community and strive to carefully reflect those inputs in the decisions made with ICANN org and Board, as an essential part of serving the public interest. However, the Board cannot accept recommendations that call for actions that are not consistent with the Bylaws-mandated policy development roles within the multistakeholder model. The Board encourages ICANN org to continue bilateral discussions with the contracted parties in a way that enhances the security, stability, and resiliency of the DNS and to strive to have these bilateral discussions be transparent to the general public, in order to continue building trust. In cases where aspects of the recommendations are not clear, the Board is placing recommendations into a pending category, directing ICANN org to seek clarifications from the SSR2 Implementation Shepherds.

Some recommendations do not clearly address a fact-based problem, or articulate what cost/benefit would be derived or how the desired outcome envisioned by the Review Team would add value and improve security, stability, and resiliency.

RySG, Namecheap, and RrSG note this as a concern in their public comments on the SSR2 Review Team Final Report. For example:

- RySG - "In an effort to create SMART recommendations the Report focuses on tactics and actions and does not include adequate problem statements to support the recommended actions."
- Namecheap - "Recommendations in the SSR2 Final Report appear to be made without any consideration of cost to ICANN. At the very least, the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine how to pay for the recommendation. Other recommendations (e.g. Recommendations 3 and 10) propose a number of ICANN initiatives (reports, participation in conferences, duplicating peer-reviewed research, etc.) that will result in significant costs - without contemplating the impact on the limited ICANN budget."
- RrSG - "Recommendations appear to have been made without any consideration of how ICANN org will pay to implement the recommendations - either through additional funding or reprioritization within the existing budget. The RrSG notes that the vast majority of ICANN's budget is ultimately paid by domain name registrants, and the Final Report does not fully explain why registrants should bear this additional burden."

In its comment on the SSR2 Review Team draft report, the Board noted that "it is helpful for the Board to have an understanding of the particular issues or risks that each recommendation intends to address...Clear articulation of the observed issue gives insight into the intent of the recommendation and the justification for why it should be adopted. With this in mind, the Board notes that a number of the SSR2 RT's recommendations, as currently drafted, do not clearly define the identified issues or risks, the rationale for the recommended solutions, the expected impact of implementation, or what relevant metrics could be applied to assess implementation." ICANN org reiterated these points in its comment on the SSR2 Review Team draft report. Throughout the review process, the Board and ICANN org also encouraged the SSR2 Review Team to consider the Operating Standards for Specific Reviews and the guidance within on how to formulate concrete fact-based problem statements. Additionally, the SSR2 Review Team took

part in the discussions between the Board and leadership of community-led review teams that led to the development of Resourcing and Prioritization of Community Recommendations: Draft Proposal for Community Discussions. The purpose of this Draft Proposal was to advance work toward principles to guide the formulation of effective community recommendations and their effective implementation, among other things.

In many cases where recommendations do not clearly address a fact-based problem, or articulate what cost/benefit would be derived or how the desired outcome envisioned by the Review Team would add value and improve security, stability, and resiliency, the Board is placing the recommendations into a pending category. The Board is directing ICANN org to complete intermediate steps including, for example, seeking clarification from the SSR2 Implementation Shepherds on what the SSR2 Review Team's intended the recommendation would mitigate, or facts that led the SSR2 Review Team to believe that the benefit would justify the cost.

Board Expectations for Next Steps

For the recommendations that the Board is placing in one of the three "pending" categories, the Board expects specific actions to take place in order to be able to take further decision on these recommendations, as noted in the Scorecard. In several cases, the Board notes that SSR2 Implementation Shepherds may be able to provide clarifications, including in connection with some of the circumstances raised in the public comments. The role of Implementation Shepherds, as detailed in the Board-adopted Operating Standards for Specific Reviews, is to be the first contact for any questions or clarifications the Board seeks as it considers the recommendations, and ICANN org seeks once the implementation is underway. Examples of information and clarification that can be sought from Implementation Shepherds include items such as the SSR2 Review Team's intent behind its recommendations; rationale for recommendations; facts that led the SSR2 Review Team to certain conclusions; and metrics related to the measure of implementation success.

The Board commits to work with ICANN org and the community toward resolving the pending status and taking appropriate action on the recommendations once the additional information is available and identified dependencies have been resolved. The Board directs the ICANN President and CEO, or his designee(s), to provide to the Board relevant information, as requested in the Scorecard, or periodic updates on progress toward gathering relevant information, starting within six months from this Board action, in order to support further Board action on each recommendation.

Prioritization of approved recommendations

Prioritization of ICANN's work is a targeted outcome of the Planning at ICANN Operating Initiative in ICANN's FY22-26 Operating Plan. It includes the design and implementation of a planning prioritization framework as part of the annual planning cycle. All Board-approved recommendations are subject to prioritization efforts. ICANN's planning process involves close collaboration among the community, Board, and organization to prioritize and effectively implement ICANN's work while ensuring accountability, transparency, fiscal responsibility, and continuous improvement. This robust planning process and the resulting plans help to fulfill ICANN's Mission.

Rationale Supporting Board Action on Individual Recommendations

Recommendations the Board approves

The Board approves thirteen (13) recommendations: 1.1, 4.1, 5.1, 5.2, 9.1, 10.1, 16.1, 21.1, 22.1, 22.2, 23.1, 23.2 and 24.2 specified in the Scorecard. Each of these recommendations is consistent with ICANN's Mission, serves the public interest, and falls within the Board's remit. Further, approved recommendations are clear, do not have dependencies - including any requiring mitigation of other work - have community support and a clear path to implementation.

Recommendation 1.1 calls for the Board and ICANN org to "perform a further comprehensive review of the SSR1 recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations." The community inputs that the Board considered when acting on Recommendation 1.1 showed that commenters generally support the recommendation. RySG and i2Coalition ask that the Board consider ongoing community work and identify areas of potential duplication or overlap when taking action on the recommendation. The Board observes that much has changed with ICANN org's processes and procedures to address review recommendations and implementation. While the SSR1 recommendations are important, assuming none of them mitigate current matters, it may be prudent for ICANN org's resources to go towards implementation of SSR2 recommendations factoring in lessons learned from SSR1.

The Board notes that further work and coordination is necessary between ICANN org and the SSR2 Implementation Shepherds to understand more clearly what can be done to consider the SSR1 recommendations fully implemented. The Board understands that ICANN org delivered to the SSR2 Review Team an assessment of implementation of the SSR1 recommendations, and that the SSR2 Review Team disagreed with many of ICANN org's assessments. However, there were no opportunities for further engagement between ICANN org and the SSR2 Review Team to explore these differences. The Board urges this type of discussion to be part of the coordination needed to implement this SSR2 recommendation. The Board also notes that the SSR2 Review Team's suggestions in Annex D of the SSR2 Review Team Final Report are to be considered by ICANN org as guidance in its review of the implementation of the SSR1 recommendations, and the suggestions are not presented as consensus recommendations of the SSR2 Review Team.

The Board approves Recommendation 1.1, subject to prioritization, risk assessment and mitigation, costing and implementation considerations. Under the Bylaws, the SSR2 Review Team is empowered to determine the extent to which ICANN org has completed implementation of the SSR1 recommendations and has done so as part of its final report. To the extent this recommendation is intended to establish a collaborative mechanism to progress implementation

of SSR2 recommendations with input from the SSR2 Implementation Shepherds, the Board approves this recommendation. The Board notes, however, that as a formal matter the Bylaws (Section 4.6(b)(iii)) reserve to SSR3 (or other future SSRs) the role of final assessment of the completion of recommendations from prior SSRs, including those that the SSR2 Review Team assessed. The Board directs ICANN's President and CEO, or his designee(s), to undertake a thorough analysis of the SSR2 Review Team's finding pertaining to the implementation of SSR1 recommendations and complete ICANN org's implementation, where appropriate, subject to prioritization, availability of resources, cost-effectiveness, and relevancy of the recommendations given the ever-changing landscape of the security, stability, and resiliency of the Internet's unique identifiers.

Recommendation 4.1 calls for "ICANN org to continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them." The community inputs that the Board considered when acting on Recommendation 4.1 showed that, in general, commenters support the recommendation and the goal of risk mitigation management.

The Board notes that ICANN org has a centralized risk management function and risk management framework in place that aligns with the ICANN Strategic Plan for Fiscal Years 2021 - 2025 and includes defined measures of success. The Board Risk Committee is responsible for the assessment and oversight of ICANN implemented policies designed to manage ICANN's risk profile, including the establishment and implementation of standards, controls, limits and guidelines related to risk assessment and risk management. The Board understands that ICANN org provided detailed information to the SSR2 Review Team with regard to risk management in the org, including via briefings and in ICANN org's comment on the SSR2 Review Team draft report.

The Board approves Recommendation 4.1, with the understanding that this recommendation is already fully implemented, and no further action is required. The Board understands that ICANN org already has policies, plans and programs in place through which Recommendation 4.1 has already been implemented, and the Board continues its oversight role over ICANN org's risk management efforts. The Board is supportive of ICANN org in continuing the risk management activities that it is already carrying out.

Recommendations 5.1 and 5.2 relate to information security management systems and security certifications. The community inputs that the Board considered when acting on Recommendations 5.1 and 5.2 showed that commenters generally support the recommendations. The Board understands that ICANN org is currently following industry-specific security standards and best practices and is in the process of migrating to the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework, with oversight from the Board Risk Committee. The Board is supportive of ICANN org continuing to migrate to the NIST Cybersecurity Framework. The Board accepts ICANN org's representation that, once migration to the NIST Cybersecurity Framework is fully complete, Recommendations 5.1 and 5.2 will be implemented. Therefore, the Board approves recommendations 5.1 and 5.2, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations, noting that substantial parts of the recommendation are already being addressed or will be addressed once ICANN org's migration to the NIST Cybersecurity Framework is fully complete.

Recommendation 9.1 calls for the Board to "direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse related obligations in contracts, baseline agreements, temporary specifications, and community policies." The community inputs that the Board considered when acting on this recommendation showed that while some community groups are in support of the recommendation, others disagree with it. For example, RySG notes the recommendation to be "extremely vague and we reiterate that ICANN's Compliance team does not need to be reminded to generally enforce

contracts with Registries and Registrars." RrSG notes that "ICANN Contractual Compliance already performs this function through complaint processing, reviews, and audits. It is not clear to the RrSG what problem this recommendation is intended to fix."

The Board notes that ICANN org's Contractual Compliance team's work already monitors and supports that registries and registrars fulfill the requirements in their agreements with ICANN org. Reporting and performance measurement metrics are published to icann.org. In addition, details regarding Registrar- and Registry-related Abuse complaints can be found in the monthly metrics published by ICANN org Contractual Compliance. This includes the number of Registrar Abuse Complaints related to pharming/phishing, malware/botnets, spam, counterfeiting, fraud, pharmaceuticals and trademark etc. as well as number of complaints related to GAC Category 1 Safeguards. As such, the Board accepts ICANN org's representation that the Contractual Compliance operations that ICANN org has in place already meet the SSR2 Review Team's defined measures of success for Recommendation 9.1. Therefore, the Board approves this recommendation, with the understanding that this recommendation is already fully implemented, and no further action is required.

Recommendation 10.1 calls for increased transparency around the working definition of DNS abuse/security threats that ICANN org uses. The community inputs that the Board considered when acting on this recommendation 10.1 showed that commenters agree that clarity around terminology and definitions of DNS abuse/security threats is important, and in general are in support of the recommended webpage. Some commenters note that existing work should be considered, for example:

- RrSG "ICANN already has a working definition of DNS abuse (see https://www.icann.org/octo-ssr/daar), and already tracks and reports on DNS abuse levels on a monthly basis."
- GNSO Council - "without a common and agreed upon definition, any additional policy work on a topic as broad as 'DNS abuse' would therefore appear extremely challenging

> and limiting the remit of any such policy related work both in scope and timeline would be a prerequisite."

To the extent that this recommendation is intended to enhance transparency, accountability, and clarity of ICANN org's work on DNS security threat mitigation through its existing contractual and compliance mechanisms, and thereby facilitate ongoing community discussions around definitions of DNS security threats, the Board approves this recommendation subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board notes that these considerations may be particularly important as definitions, procedures and protocols may evolve over time. In this regard, the Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ICANN org's Information Transparency Initiative (ITI).

Recommendation 16.1 calls for ICANN org to "provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the RDS." The Board approves Recommendation 16.1, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ITI.

Recommendation 21.1 pertains to security of ICANN org and Public Technical Identifiers (PTI) communications with Top-Level Domain operators. **Recommendations 22.1 and 22.2** pertain to metrics on the availability of services provided by ICANN org, including root-zone and gTLD-related services as well as Internet Assigned Numbers Authority (IANA) registries. **Recommendations 23.1 and 23.2** pertain to preparations for future root DNSKEY algorithm rollovers.

The community inputs that the Board considered when acting on Recommendations 21.1, 22.1, 22.2, 23.1 and 23.2 showed that commenters generally support these recommendations. The Board notes that efforts to implement the new Root Zone Management System are already underway and the Board is supportive of building on existing efforts to enhance security in the Root Zone System. The Board notes that Recommendation 23.2 must be completed before the DNSSEC Practice Statement can be updated as called for in Recommendation 23.1. Further, the Board notes that preparing for an algorithm roll is part of the PTI Strategic Plan. As such, some elements of work associated with these recommendations are already anticipated to take place. The Board approves Recommendations 21.1, 22.1, 22.2, 23.1 and 23.2, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations.

Recommendation 24.2 recommends that ICANN org "make the Common Transition Process Manual easier to find by providing links on the EBERO (Emergency Back-end Registry Operator) website." The community inputs that the Board considered when acting on Recommendation 24.2 showed that commenters generally support this recommendation. The Board approves recommendation 24.2, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ITI.

Recommendations the Board rejects because the recommendation cannot be approved in full.

The Board rejects six recommendations because the recommendations cannot be approved in full: 4.2, 8.1, 9.4, 10.2, 10.3 and 17.2. In the case of these recommendations, the Board notes that, while some portions of the recommendation could be feasible, and in some cases, work is already underway, there are limitations imposed by other portions of the same recommendation that could impact feasibility. While the Board agrees in principle with the intent of many of these recommendations, the Board does not have the option of selectively approving some parts and rejecting other parts of a single, indivisible community recommendation and must act on a

recommendation as written and not as interpreted by ICANN org or the Board. As such, the Board rejects these recommendations. However, the Board further notes that it may wish to direct action from ICANN org on some of the ideas within the recommendations. Such actions would not be tracked as part of the tracking of the implementation of SSR2 recommendations.

Recommendation 4.2 calls for ICANN org to adopt and implement ISO 31000 for risk management. The Board notes that ICANN org has a centralized risk management function and risk management framework in place that is based on the most commonly accepted best practices set by the COSO framework and aligns with the ICANN Strategic Plan for Fiscal Years 2021 - 2025 and includes defined measures of success. As ICANN org noted in its comment on the SSR2 Review Team draft report the main elements and outcomes of ISO 31000 are included in ICANN org's risk management framework. Under the framework, ICANN org uses its own in-house resources to achieve the same outcomes in a fit-for-purpose way.

The Board Risk Committee (BRC) is responsible for oversight of ICANN implemented policies designed to manage ICANN's risk profile, including the establishment and implementation of standards, controls, limits and guidelines related to risk assessment and risk management. The BRC most recently reviewed the status of the risk management target model (Model) during its 13 April 2021 meeting. The Model was developed in 2014-2015 by ICANN org, the BRC, and external consultants, and agreed by the Board. ICANN org's then Risk Management program was benchmarked to the Model and the gaps identified. Over the past few years, ICANN org has worked to close those gaps. The community inputs that the Board considered when acting on Recommendation 4.2 showed that, in general, commenters support the goal of risk mitigation management.

The Board also agrees in principle that ICANN org should have "a strong, clearly documented risk management program" and follow international standards, as noted in the SSR2 Review Team's measures of success for Recommendations 4.1 - 4.3. In fact, the Board notes that ICANN org has a centralized risk management function and risk management framework in

place that is based on the most commonly accepted best practices and that a Board committee is responsible for oversight of ICANN implemented policies designed to manage ICANN's risk profile. The Board notes that ICANN org has a strong, clearly documented risk management program, but not as envisioned by SSR2, as written. Thus, the Board agrees with the recommendation in principle, and considers the intent of the recommendation achieved through ICANN org's current operations. However, the Board cannot approve the portion of the recommendation that specifies that ICANN org "adopt and implement ISO 31000 'Risk Management' and validate its implementation with appropriate independent audits…" because it is not clear what risks would be mitigated , nor what benefit would be derived in expanding significant resources to switch from the current risk-management process.

The Board supports ICANN org's risk management operations already in place. In light of the above considerations, and the fact that approval of the recommendation would require ICANN org to adopt and implement ISO 31000, while the Board agrees in principle with the intent of the recommendation, the Board rejects recommendation 4.2. The Board encourages ICANN org to continue following industry best practices and look for ways to strengthen its risk management practices as it evolves its operations as part of its continuous improvement.

Recommendation 8.1 calls for ICANN org to "commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the domain name system for end-users, businesses, and governments."

The community inputs that the Board considered when acting on this recommendation showed that while some community groups are in support of the recommendation as written, others disagree with the recommendation, or elements of the recommendation. The Board notes that many of those disagreeing with this recommendation are parties to the contracts at issue, and identified that the recommendation is not appropriate under existing contracts. For example:

- RySG, PIR, Tucows, Namecheap, and RrSG note concerns that the recommendation is not consistent with the terms of the Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA).
- GAC - "GAC agrees with the spirit of the recommendation, but recognises that "contract negotiations between ICANN and the Contracted Parties do not currently include third parties and therefore would encourage ICANN to consult with independent security experts (i.e. non-contracted entities) for the purposes of developing and agreeing upon security-related provisions that can be incorporated into the contracts."

The Board notes that the aspect of the recommendation that calls for the introduction of a third party into the bilateral negotiation process is not proper or feasible. The RA[2] and RAA[3] do not allow for third-party beneficiaries[4,5]. The Board notes that ICANN org negotiates in the broader interest of ICANN, including the public interest, and does not represent the interests of the domain industry. The Board also understands that parts of the ICANN community have concerns, as reflected through the public comments, about how Contracted Party agreements are negotiated, and acknowledges that it is important to listen carefully to the community as negotiations proceed and decisions are made. ICANN org also has an important enforcement role once items are incorporated into contracts.

The Board further notes that recommendation 8.1 is not allowed under the provisions of the RA and RAA. While the agreements do provide for a "Working Group", these have contractually specific meanings that are not aligned with this recommendation. For example, in the case of the RA, a "Working Group" is defined as: "representatives of the Applicable Registry Operators and

---

[2] Base Registry Agreement - Updated 31 July 2017. Section 7.7: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

[3] 2013 Registrar Accreditation Agreement. Section 7.4: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa

[4] Base Registry Agreement - Updated 31 July 2017. Section 7.8: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

[5] 2013 Registrar Accreditation Agreement. Section 7.5: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa

other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements (excluding bilateral amendments pursuant to Section 7.6(i)).”[6] Neither the Board or ICANN org is involved in the appointment of these contractual “Working Groups”.

Further, as the Board and ICANN org noted in their respective comments on the SSR2 Review Team draft report, the Board and ICANN org cannot bring about contractual changes unilaterally. If changes in provisions of the contracts are desired in order to address perceived gaps related to security, stability, and resiliency of the DNS for end-users, businesses, and governments, as referred to in Recommendation 8.1, then the Policy Development Process allows for such “independent experts” as mentioned in the recommendation to participate as those policy recommendations are developed.

In light of the above considerations, the Board rejects this recommendation. The Board encourages ICANN org to continue bilateral discussions with the contracted parties in a way that enhances the security, stability, and resiliency of the DNS and to strive to have these bilateral discussions be transparent to the general public, in order to continue building trust.

Recommendation 9.4 calls for ICANN org to “task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.” The community inputs that the Board considered when acting on this recommendation showed that while some community groups are in support of the recommendation, others note concerns with recommendations in the SSR2 Review Team Final Report related to ICANN org’s Contractual Compliance team that are applicable to this recommendation. For example:

[6] Base Registry Agreement - Updated 31 July 2017. Section 7.6(j)(v): https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

- RySG - "The implication of Recommendation 9 is that ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement. The Registries disagree with this characterization and note that Registry Operators' compliance with their abuse obligations were recently audited by ICANN Compliance."
- PIR - "Some recommendations imply that ICANN Compliance is not enforcing existing contractual obligations or encourage ICANN Compliance to undertake activities that are clearly outside of ICANN Compliance's scope and remit."

The Board notes that ICANN org's Contractual Compliance operations already in place ensure that registries and registrars fulfill the requirements in their agreements with ICANN org. Through the Contractual Compliance team, ICANN org enforces policies that have been adopted by the community and makes operational and structural changes as needed to carry out its enforcement role. ICANN org's Contractual Compliance team cannot serve in a proactive policy development capacity.

The Board accepts in principle the idea of improving the tools that the ICANN org Contractual Compliance team has available to it in order to enforce policies that have been adopted by the community. However, the Board cannot approve the part of the recommendation that contemplates "measures that would require changes to the contracts" as such changes cannot be undertaken by either the Board or ICANN org unilaterally. As such, the Board rejects this recommendation given that it is not consistent with the role and authority of ICANN org's Contractual Compliance team. The Board encourages ICANN org's Contractual Compliance team to continue pursuing new tools that will help improve its work.

Recommendations 10.2 and 10.3 call for establishment of a cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, and for the Board and ICANN org to use the consensus definitions consistently. The community inputs that the Board considered when acting on this recommendation showed that in general, commenters

agree that clarity around terminology and definitions of DNS abuse is important but have some concerns or caveats about the recommendation. For example,

- RySG - " RySG would welcome a culture of open discussions aimed at further evolving the definitions of DNS Abuse in the future, as suggested in Recommendation 10.2. We would, however, recommend acknowledging the traditional stakeholders in a CCWG, including Contracted Party representatives, in the recommendation, in addition to the stakeholders named."
- GNSO Council - "Without expressing an opinion on the formation of a CCWG, the GNSO Council asks the ICANN Board to consider present and near-term demands of other policy work on the ICANN Org, staff, and larger ICANN community. Without a common and agreed upon definition, any additional policy work on a topic as broad as 'DNS abuse' would therefore appear extremely challenging and limiting the remit of any such policy related work both in scope and timeline would be a prerequisite."
- RrSG - "Formation of a CCWG as described in this recommendation is outside of the ICANN Bylaws and the GNSO Operating Procedures. Additionally, the directions are overly prescriptive, do not allow for realistic timelines, and do not clearly state the problem that the recommendation is attempting to solve."

The Board rejects Recommendation 10.2, as neither ICANN org nor Board can unilaterally establish a CCWG. A CCWG is a mechanism created by the community to facilitate collaborative work on topics that have been identified as not being within the remit of a specific Supporting Organization or Advisory Committee. Although there is no mandatory process governing the creation or operation of a CCWG, the ccNSO and GNSO communities developed a Uniform Framework for Principles & Recommendations for CCWGs in 2016 that clarifies the views of two of ICANN's policymaking bodies regarding the circumstances and scope for which a CCWG is appropriate.

However, the Board notes that the community continues its discussions over DNS security threat mitigation. Discussions include questions around the definitions and scope of DNS security

threats that can be considered as coming within ICANN's remit and the extent to which policy or other community work may be required to supplement efforts already underway, such as industry-led initiatives. The Board is fully supportive of this effort and remains committed to this important work through facilitation and the convening of diverse relevant groups with diverse viewpoints.

The Board rejects Recommendation 10.3 due to its dependencies on Recommendation 10.2; however, the Board supports using consensus definitions consistently.

Recommendation 17.2 asks the ICANN community to develop a policy for avoiding and handling new gTLD-related name collisions. The community inputs that the Board considered when acting on this grouping of recommendations showed that while some community groups support the recommendation, others disagree with it. For example, while IPC supports the recommendation, it notes that IPC "has diverse opinions on Name Collision." RySG, IPC, and Article 19 express concerns that this recommendation overlaps with or is in contradiction to the ongoing work related to Name Collision. For example:

- Article 19 - "While we welcome the recommendation, we urge that the section is redrafted so that it is not in contradiction with the recommendations outlined under the GNSO New Subsequent Procedures Draft Final Report. We specifically note that the recommendation heavily relies on the Name Collision Analysis Project (NCAP) Studies I without reference to the rest of the ongoing work carried out by the NCAP studies group including NCAP Studies II and III. In this regard, we would like to reiterate our recommendations submitted to the GNSO New Subsequent Procedures Working Group in September 2020 (comments which are still applicable in the current March 2021 situation), where we stated that, '...We welcome the work of the Working Group regarding this topic and support all the affirmations and recommendations as written, especially on the use of the New gTLD Collision Occurrence Management framework. At this time, we do not support the replacement of this framework by a new Board approved framework that may result from the Name Collision Analysis Project (NCAP)

> Studies I, II and III. Any proposal for a new mitigation framework would be premature given the work of the NCAP studies group is yet to be completed….'. We would thus like to recommend that recommendation 17 is revised to note that measuring name collisions should be carried out under the ongoing framework pending full completion of the work carried out by the NCAP studies group."

On 2 November 2017 the Board passed resolutions 2017.11.02.29 – 2017.11.02.31 requesting that the Security and Stability Advisory Committee (SSAC) conduct a study to facilitate the development of policy on collision strings to mitigate potential harm to the stability and security of the DNS posed by delegation of such strings. The SSAC proposed a series of three studies, and an independent contractor completed the Name Collision Analysis Project (NCAP) Study 1 in June 2020, which included consideration of input received through two Public Comment proceedings. Subsequently, the community-based NCAP Discussion Group redesigned the proposal for NCAP Study 2 and on 25 March 2021 the Board passed resolutions 2021.03.25.11 – 2021.03.25.14 affirming the continued relevance of the nine questions related to name collisions presented in the prior Board resolutions 2017.11.02.29 - 2017.11.02.31, especially questions concerning criteria for identifying collision strings and determining if collision strings are safe to be delegated. The Board also directed the NCAP Discussion Group to proceed with NCAP Study 2 as redesigned.

In addition, the Board has received the Final Report from the GNSO's Policy Development Process on New gTLD Subsequent Procedures, which contains a recommendation and additional implementation guidance on the topic of name collisions. The Board understands that the GNSO Council affirms that the New gTLD Collision Occurrence Framework should continue to be used until a new framework is developed and adopted. The Board notes that, while the GNSO Council's PDP outcomes contemplate the possibility that further community work may be needed, the Final Report was completed prior to the Board's approval to move forward with NCAP Study 2 and that the GNSO Council in approving the PDP outcomes also requested that "the ICANN Board consider and direct the implementation of the Outputs adopted by the GNSO

Council without waiting for any other proposed or ongoing policy work unspecific to New gTLD Subsequent Procedures to conclude, while acknowledging the importance of such work."

Further, the Board notes that, while it can request an Issue Report and require the initiation of a PDP in the GNSO, and EPDP can only be launched by a GNSO Council vote, and only in specific circumstances ("to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the ICANN Board or the implementation of such an adopted recommendation; [or] to provide new or additional policy recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists"[7]).

In light of the above considerations, the Board rejects Recommendation 17.2, as the Board does not have the authority to develop policy. The Board notes that the community has already conducted extensive policy work concerning the process for handling name collisions for the next round of new gTLDs, and NCAP is another significant community effort already underway that is expected to result in additional useful information for the Board and community on the topic. Given the ongoing work in this area, including the NCAP studies, the Board understands that the results of those studies may have implications for SSR in the context of a future round of New gTLDs.

Recommendations the Board rejects

The Board rejects ten (10) recommendations: 2.1, 2.2, 2.3, 2.4, 14.1, 14.3, 14.4, 14.5, 15.1, and 15.2.

Recommendations 2.1, 2.2, 2.3 and 2.4 recommend that ICANN org "create a C-suite position responsible for both strategic and tactical security and risk management." The Board notes that

[7] GNSO Operating Rules and Procedures: Annex 4 - Expedited Policy Development Process Manual: https://gnso.icann.org/sites/default/files/file/field-file-attach/2016-12/annex-4-epdp-manual-01sep16-en.pdf

implementation of Recommendations 2.2, 2.3 and 2.4 are dependent on implementation of Recommendation 2.1, and as such the Board takes action on these recommendations as a group. The community inputs that the Board considered when acting on these recommendations show that, while some community groups express support, RySG, i2Coalition, Namecheap, and RrSG note that the work specified in the role description is already being carried out by members of ICANN org, and as such do not support the recommendation. For example:

- RySG - "RySG supports these recommendations insofar as they represent strategic requirements for ICANN Org risk management. We do not support the creation of the new function to oversee security and risk management, as suggested per Recommendation 2.1., as we believe that these roles can (and currently are being) handled by existing members across different functional areas within ICANN Org, including OCTO."
- Namecheap - "Recommendations 2, 3, and 4.3 already exist within ICANN. John Crain has the title of Chief Security, Stability & Resiliency Officer. Mr. Crain (and his team) are part of the Office of the Chief Technology Officer (OCTO)- which has approximately twenty members. Mr. Crain and OCTO already have a transparent budget, conduct (and publish) extensive research, and participate in many ICANN and industry forums. The OCTO team has an extensive list of publications at https://www.icann.org/octo. It is not clear from the SSR2 Final Report whether the Review Team is aware of these ICANN activities, or how the Review Team finds these significant and beneficial activities to be insufficient."

In their respective comments on the SSR2 Review Team draft report, the Board and ICANN org encouraged the SSR2 Review Team to provide specific details as to what issues or risks the SSR2 Review Team had identified with the current operations, how the SSR2 recommendation will address these issues or risks, and what relevant metrics could be applied to assess implementation. The SSR2 Review Team did not provide the further requested information in the SSR2 Review Team Final Report.

The Board notes that it has an oversight role; it is the responsibility of the ICANN President and CEO to structure ICANN org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability.

Further, ICANN org is in a relatively unique state in regard to security management. There is the traditional role of data and systems security that most organizations have and protect against as well as the security and well-being of its staff. However, since ICANN org facilitates numerous meetings of scale with its communities and holds a particular role in managing portions of the Internet's unique identifier systems as defined in its Bylaws, which are both different types of physical and data security, ICANN org felt that the scope to be too big and the breadth too diverse to manage these distinctly different functions under one reporting structure. ICANN org noted this in its comment on the SSR2 Review Team draft report. As the organization matured over the years, it became clear that these security-related functions would be best managed in a distributed manner with specific and narrow responsibilities to be managed by the executive of the functional team best suited for each specified role. This decision was not made lightly, and ICANN org continues to evaluate and refine where these responsibilities lie. The Board supports ICANN org's decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN org is responsible.

In addition, also as noted in its comment on the SSR2 Review Team draft report, ICANN org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-Suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. The CEO Risk Management Committee

is therefore a mechanism that provides ICANN org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures that ICANN org intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost.

In light of the above considerations, the Board rejects Recommendations 2.1, 2.2, 2.3 and 2.4. However, the Board agrees with increased reporting and periodic communication of SSR activities. This is already partially performed as part of the current annual planning process but could be enhanced consistently with the presumed intent of the Recommendation 2.2.

Recommendations 14.1, 14.3, 14.4, 14.5, 15.1 and 15.2 relate to creating a Temporary Specification and launching an Expedited Policy Development Process (EPDP) for evidence-based security improvements. The Board notes that the SSR2 Review Team Final Report addresses these recommendations together in terms of the defined measures of success[8]. The community inputs that the Board considered when acting on this grouping of recommendations showed that, in general, while community groups are supportive of evidence-based security improvements and believe efforts related to improvements to be high priority, several community groups note concerns with the recommendations as written. RySG, Tucows, PIR, and RrSG note concerns that this grouping of recommendations does not meet the threshold for establishing a Temporary Specification, or requirements for launching an EPDP. For example:

- RySG - "Recommendation 14 fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways: (1) The Recommendation fails to meet the requirement that a temporary specification be as 'narrowly tailored' as feasible to achieve its defined purposes; and (2) Temporary Specifications must address an immediate need to preserve

[8] SSR2 Review Team Final Report (p46): https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues."

- Tucows - "Tucows supports SSR2's commitment to evidence-based improvements but is not clear on why a Temporary Specification is recommended rather than a standard PDP. The SSR2 does not make clear why this might be an emergency of the type envisioned by the IANA transition team; in the absence of such clarity, a standard PDP is the appropriate choice. Furthermore, the Tucows family of registrars notes that DNS Abuse has objectively decreased, as evidenced by data collated and published by ICANN itself as 'Identifier Technology Health Indicator' metrics. The SSR2 does not take this into account, which unfortunately detracts from the good recommendations it has. Any policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context."
- RrSG - "The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA. This recommendation fails to identify the background necessitating additional requirements on registrars and registries without their participation in creating such a Temporary Specification."

The Board notes that Temporary Policies can only be established by the Board upon specific requirements, such as when the Board "reasonably determines that such modifications or amendments are 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, the DNS or the Internet"[9,10]. The Board notes that Recommendation 14.1

[9] Base Registry Agreement - Updated 31 July 2017. Section 2: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

[10] 2013 Registrar Accreditation Agreement 'Consensus Policies and Temporary Policies Specification':https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary

does not provide such emergency grounds, and as such rejects this recommendation and the recommendations dependent on its implementation (14.3, 14.4, 14.5, 15.1 and 15.2).

Further, the Board notes that, while it can request an Issue Report and PDP be done by the GNSO, an EPDP can only be launched by a GNSO Council vote, and only in specific circumstances ("to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the Board or the implementation of such an adopted recommendation; [or] to provide new or additional policy recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists"[11]). The Board notes that Recommendation 15.1 does not meet these requirements. The Board, consistent with its action on the Competition, Consumer Trust, and Consumer Choice (CCT) Review Team recommendations, will not take the place of the community within the multistakeholder model and initiate a PDP upon a Specific Review team's recommendation. As such, even without dependency on Recommendation 14.1, the Board would not be in a position to approve Recommendations 15.1 and 15.2.

Recommendations that the Board determines to be pending, likely to be approved once further information is gathered to enable approval.

The Board places four recommendations (5.4, 19.1, 19.2 and 20.2) into "pending, likely to be approved once further information is gathered to enable approval", in light of the considerations noted below. As specified in the Scorecard, the Board expects specific actions to take place in order to take further Board decision on these recommendations. The Board uses this category to communicate to the ICANN community that based on the information available to date, the Board anticipates that each of these recommendations will be approved. The community inputs that the Board considered when acting on these recommendations showed that commenters generally support these recommendations.

[11] GNSO Operating Rules and Procedures: Annex 4 - Expedited Policy Development Process Manual: https://gnso.icann.org/sites/default/files/file/field-file-attach/2016-12/annex-4-epdp-manual-01sep16-en.pdf

Recommendation 5.4 calls for ICANN org to "reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space including information describing how ICANN org follows continually improving best practices and process to manage risks, security and vulnerabilities." While implementation of the recommendation appears feasible, the Board requires clarification on several elements of this recommendation in order to accurately assess resource requirements and enable approval. For example, the required granularity of the reports expected by the SSR2 Review Team, and what entities the SSR2 Review Team envisioned ICANN org report out to "beyond" the ICANN community are not clear. The Board directs the ICANN President and CEO, or his designee(s) to seek clarifications from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendation 5.4 can be approved.

Recommendations 19.1 and 19.2 recommend that ICANN org should "complete the development of a suite for DNS resolver behavior testing" and "ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained." The Board notes that the SSR2 Review Team's discussion and recommendations in the Final Report refer to three different things: a "DNS testbed"; a "regression test suite"; and "a suite for DNS resolver behaviour testing." While any of these may be feasible, the Board requires clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent in order to accurately assess resource requirements. The Board directs the ICANN President and CEO, or his designee(s), to seek clarifications from the SSR2 Implementation Shepherds on elements of these recommendations that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendations 19.1 and 19.2 can be approved. Further, the Board understands that the testbed would operate indefinitely so as to be applicable to future changes in resolvers. If the Board eventually approves this

recommendation, maintenance of a testbed environment would have to be a persistent budget item in all future budget cycles for continued development and upkeep.

Recommendation 20.2 calls for ICANN org to "create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root Key Signing Key (KSK) rollover process." While the recommendation appears feasible and the Board believes that table-top exercises would be beneficial, more information is needed to understand what the SSR2 Review Team intended to be targeted in the table-top exercises following the Root KSK rollover process. The Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendation 20.2 can be approved.

Recommendations the Board determines to be pending, holding to seek clarity or further information.

The Board places twenty-four (24) recommendations into "pending, holding to seek clarity or further information": 3.1, 3.2, 3.3, 4.3, 5.3, 7.1, 7.2, 7.3, 7.5, 9.3, 11.1, 12.1, 12.2, 12.3, 12.4, 13.1, 13.2, 14.2, 17.1, 18.1, 18.2, 18.3, 20.1 and 24.1. The Board is unable to signal at this time whether it is likely to accept or reject each of these recommendations pending the collection of additional information.

Recommendations 3.1, 3.2 and 3.3 pertain to responsibilities of the C-Suite position recommended in Recommendation 2 and SSR-related budget transparency. The community inputs that the Board considered when acting on this recommendation showed that while several commenters support the recommendations, RySG, i2Coalition, Namecheap, and RrSG believe that the recommendations are already being addressed, or can be sufficiently addressed within

the current ICANN organization structure, without the addition of a C-Suite level position. For example:

- RySG - "RySG supports the recommended actions to improve SSR-related budget transparency, but cautions that briefings to the ICANN community on SSR strategy and projects should be high level and not disclose specific security practices, so as not to introduce potential attack vectors. We reiterate that, as per our previous comment, we do not support the creation of the Executive CSuite Security Officer referred to in Recommendation 3.1, as this role is already sufficiently being covered within ICANN Org."
- i2Coalition - "The Final Report is full of recommendations that, without stating the problem that is to be solved, ask for new roles that already seem to exist (2.1, 3.1, 4.3), or seem to be pushing ICANN into the realm of policing DNS protocols (19). This is a serious concern with recommendations that, once accepted by the Board, would create duplicative work, or even seem to expand ICANN's remit."
- Namecheap - "A number of the recommendations in the SSR2 Final Report address items or functions that ICANN org already provides- and in some cases is already dedicating significant resources toward. Specifically, Recommendations 2, 3, and 4.3 already exist within ICANN."
- RrSG - "It is not clear to the RrSG how ICANN's current public comment on its budget (including SSR-related items) and strategic planning is deficient to necessitate this recommendation, nor why the Review Team designated this as a high priority item."

The Board supports increased transparency where possible, and as such agrees with the intent of these recommendations. ICANN org is already undertaking work towards improving budget transparency. For example, ICANN org's Operating and Financial Plans for FY22-26 (Five-Year) and FY22 (One-Year), includes "Appendix C: ICANN Security, Stability, and Resiliency (SSR) of the Unique Internet Identifiers". This appendix states: "ICANN's deep commitment to SSR underscores an approach to the concept that is holistic and interwoven into daily operations. In other words, every function of ICANN org contributes to the overall SSR through its support

of org's work to advance ICANN's Mission. However, this Appendix aims to articulate some of the specific areas that particularly focus on supporting the SSR of these unique Internet identifiers."

Further, the Board agrees with the benefit of a process of periodic communication on SSR activities and notes this is already partially performed as part of the current annual planning process. The Board encourages ICANN org to continue enhancing its periodic communication on SSR activities as part of its work and operations.

However, the Board notes that, as written, successful implementation of Recommendations 3.1 - 3.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation.

In light of the above considerations, the Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent, and if implementation of these recommendations can be considered effective after the Board rejects Recommendation 2, thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendations 3.1, 3.2, and 3.3 to that new office. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendation 4.3 recommends that ICANN org "name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role" as recommended in Recommendation 2. The community inputs that the Board considered when acting on Recommendation 4.3 showed that while several commenters support the recommendation, RySG, i2Coalition, Namecheap, and RrSG cite concerns about the elements of

the recommendation that ask for a new role to be created that already exists in ICANN org. For example:

- RySG - "RySG is generally supportive of risk mitigation management within ICANN and believe that this can be sufficiently addressed within the current ICANN staff structures without the addition of a C-Suite level position."
- i2Coalition - "The Final Report is full of recommendations that, without stating the problem that is to be solved, ask for new roles that already seem to exist (2.1, 3.1, 4.3), or seem to be pushing ICANN into the realm of policing DNS protocols (19). This is a serious concern with recommendations that, once accepted by the Board, would create duplicative work, or even seem to expand ICANN's remit."
- Namecheap - "Recommendations 2, 3, and 4.3 already exist within ICANN…It is not clear from the SSR2 Final Report whether the Review Team is aware of these ICANN activities, or how the Review Team finds these significant and beneficial activities to be insufficient."
- RrSG - "As of the date of this comment, ICANN's Office of the Chief Technology Officer (OCTO) comprises approximately 20 staff. It is not clear to what extent the functions identified in this recommendation are not currently performed by OCTO, or why a new position is required to perform these functions. To the extent these functions are not currently performed by OCTO, the team should be capable of incorporating these items into their existing departmental structure."

The Board notes that as written, successful implementation of Recommendation 4.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. In light of this dependency on Recommendation 2, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective after the Board rejects Recommendation 2 thereby removing the possibility of assigning

the additional roles or responsibilities as called for in Recommendation 4.3. The Board has a concern with accepting a recommendation for which implementation can never be deemed successful or effective.

Further, the Board notes it is the responsibility of the ICANN President and CEO, or his designee(s), to structure ICANN org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability. In addition, it is not clear as to what the SSR2 Review Team envisioned would be mitigated, nor what cost/benefit would be derived from the recommended structure.

The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendation 5.3 recommends "external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers." The community inputs that the Board considered when acting on Recommendation 5.3 showed commenters generally support the recommendation. The Board understands that ICANN org's Engineering & Information Technology (E&IT) function already requires all vendors and service providers to have a risk assessment performed and documented which meets industry-standard requirements. In order to accurately assess resource requirements and feasibility, the Board requires clarification from the SSR2 Implementation Shepherds as to if the SSR2 Review Team's intent was to expand this risk assessment to all ICANN org vendors and service providers. The Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherd as to the SSR2 Review Team's intended scope of this recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendations 7.1, 7.2, 7.3 and 7.5 pertain to business continuity and disaster recovery processes and procedures. The community inputs that the Board considered when acting on Recommendations 7.1, 7.2, 7.3 and 7.5 showed that most commenters are in support of the recommendations, however RySG notes some concerns:

RySG - "While the RySG supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan, the proposed scope of 'all the systems owned by or under the ICANN org purview' is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes. Similar, for example, to the IANA risk management strategy for its services. We recommend that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators."

The Board notes that the SSR2 Review Team states successful measures of implementation for these recommendations as: "This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational."[12] The Board is placing Recommendation 7.4, which calls for the "non-U.S., non-North American site" into "pending, likely to be rejected unless additional information shows implementation is feasible."

As such, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of these recommendations can be considered effective in the event that the Board rejects

[12] SSR2 Review Team Final Report (p30): https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

Recommendation 7.4 regarding opening a non-U.S., non-North American site, and that portion of the success measure cannot be achieved. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective.

The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendation 9.3 recommends that ICANN org has "compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans." The community inputs that the Board considered when acting on Recommendation 9.3 showed that most commenters support the recommendation, although RySG and RrSG note some concerns. For example:

- RySG - "The implication of Recommendation 9 is that ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement. The Registries disagree with this characterization and note that Registry Operators' compliance with their abuse obligations were recently audited by ICANN Compliance.
- RrSG - "Any audit of Contractual Compliance should focus on its structure, staffing, activities, systems, processes, and the overall efficiency and effectiveness of this function. Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing."

The Board notes that some elements of this recommendation are not clear, such as what would be audited, against what criteria, by whom, or why an external auditor would be required. The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the SSR2 Implementation Shepherds on elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendation 11.1 pertains to the availability of Centralized Zone Data Service (CZDS) data. The community inputs that the Board considered when acting on this recommendation

showed that while some community groups are in support of the recommendation, others express concerns. For example:

- RySG - "The current CZDS system not only provides sufficient access but was also the result of lengthy negotiations taking into account the varying needs of different members of the ICANN community, including the registries that provide this access."
- NCSG - "Brand protection and intellectual property protection are not security and stability issues. But in this section 'brand protection' is again invoked. This is a risky path to take and can lead to extending the ICANN mission and the definition of DNS abuse."

The Board notes that some elements of this recommendation are not clear. For example, the Board notes that ICANN org is currently in the process of implementing recommendations from SAC097, which calls for ICANN org to revise "the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default." It is not clear what additional work is needed to sufficiently implement the SSR2 Review Team's Recommendation 11.1 or how the existing work already being performed on CZDS access is insufficient. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendations 12.1, 12.2, 12.3, 12.4, 13.1 and 13.2 pertain to transparency and accountability of DNS abuse analysis and reporting efforts, and complaint reporting. The community inputs that the Board considered when acting on this recommendation showed that while several community groups support the recommendations, others have some concerns. For example, with regard to Recommendations 12.1, 12.2, 12.3 and 12.4:

- RySG - "ICANN Org has produced DAAR as a means of informing the community of the apparent existence of DNS Abuse. There are other organizations that produce similar

types of reports within the context of their own mission and purpose. The RySG's DNS Abuse Working Group (and its predecessor the DAAR Working Group) has been working collaboratively with OCTO to ensure that DAAR provides the community with the best information available. Without a stated objective or observable problem this recommendation prescribes a solution with dubious value...Specifically, the notion of a time-delay in data-sharing is antithetical to the goal of mitigating abuse as quickly as practical and would appear to be competitive with ICANN Org's compliance responsibilities that also occur after-the-fact."

- Article 19 - "We caution that any process of dealing with DNS abuse should be done through a public consultation process and should not expand ICANN's mandate beyond infrastructure to include content regulation."
- Tucows - "Any attempt to identify Contracted Parties that 'contribute to abuse' is fraught with impossibility: mere numbers and percentages do not tell the whole story. The Tucows family of registrars notes the good work of the Registrar of Last Resort, for example, as well as the fact that the majority of abuse occurs in the .com registry—which speaks to its popularity, not to its permissive or welcoming nature towards abusive registrations. The problems with Recommendation 12.3 should be obvious but, to avoid doubt: attempting to identify registries and registrars that 'contribute to abuse' by quantifying the number of abusive registrations or clients on their platform instead simply indicates a high-volume business. Instead, attention should be given to business practices which allow for abusive behaviour or clients with indicators of abusive intent."
- NCSG - "DAAR was never set up for the purpose of auditing registries and registrars. It is not a 'punishment mechanism' but a research mechanism. It should never have a mission such as identification of registries and registrars that harbor a disproportionate level of abuse. DAAR was recommended by GAC in multiple communiques and it provides useful statistics that can be helpful for security research. So it should not be discontinued at the request of the review team but the community as a whole should decide which direction it should take."

- RrSG - "ICANN already operates the DAAR, and it is not clear what limitation or oversight this recommendation intends to address. Without identifying the specific deficiencies, the Review Team should not instruct ICANN to spend significant money to accomplish unidentified goals.

The Board acknowledges the extensive community and ICANN org efforts currently going on around DNS security threats.

The Board directs the ICANN President and CEO, or his designee(s), to evaluate how this grouping of recommendations, along with other recommendations that pertain to DNS security threats should be considered in a coordinated way, including through ICANN org's program dedicated to DNS security threats mitigation. This information will inform the Board's decision on next steps. The Board notes, however, that beyond the interdependencies related to the extensive community and ICANN org efforts around DNS security threats, there may be additional challenges associated with implementation of some of these recommendations that the Board would require to be addressed before determining if these recommendations can be approved.

Recommendation 14.2 recommends that ICANN org provide contracted parties with lists of domains in their portfolios identified as abusive to enable anti-abuse action. While the Board is rejecting Recommendations 14.1, 14.3, 14.4 and 14.5 for specific reasons, the Board recognizes that recommendation 14.2 appears to be independent from these recommendations.

The community inputs that the Board considered when acting on this recommendation showed that, while commenters offer mixed views about other recommendations in the Recommendation 14 grouping, specific comments about recommendation 14.2 are more limited. GAC notes that "CCT Review Recommendation 12 also saw value in the financial incentivisation (SSR2 Recommendation 14.5) of contracted parties encouraging them to reach certain DNS Abuse milestones. Such financial incentives, of course, are only possible when there first exists a shared

understanding of which domains within a contracted party's portfolio are perceived to be abusive (SSR2 Recommendation 14.2)." RySG specifically notes it "does not object to Recommendation 14.2", while RrSG notes "The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse. If third parties have concerns or identify specific and verifiable cases of abuse, they should report them to the appropriate contracted party."

The Board notes that ICANN org currently measures specific security threats related to domain names through several projects, including the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project, and Domain Abuse Activity Reporting System (DAAR), both of which have a publication or reporting element.

The Board understands that all such projects rely on commercially licensed data that come with varying restrictions on what data can be shared and how. Through the DNSTICR, ICANN org produces reports on recent domain registrations that ICANN org understands to be using the COVID-19 pandemic for phishing or malware campaigns. These reports, which are shared with the responsible parties (primarily registrars or registries), contain the evidence that leads ICANN org to believe the domains are being used maliciously, along with other background information to help the responsible parties determine the correct course of action.

The overarching purpose of DAAR is to develop a robust, reliable, and reproducible methodology for analyzing security threat activity, which the ICANN community may use to make informed policy decisions. The system collects TLD zone data and complements these data sets with a large set of high-confidence Reputation Block List (RBL) security threat data feeds. The aggregated statistics and anonymized data collected by the DAAR system can serve as a platform for studying, reporting daily, or historically the registration data, or the abuse activity by each registry. This aggregated data is currently pushed to the registries using ICANN's Service Level Agreement Monitoring (SLAM) system.

The Board directs the ICANN President and CEO, or his designee(s) to regard the measures of success as defined by the SSR2 Review Team for Recommendations 14 and 15, and evaluate how this recommendation, along with other recommendations that pertain to DNS security threats, should be considered in a coordinated way, including through the ICANN org program dedicated to DNS security threats mitigation and ongoing projects such as DNSTICR and DAAR. This information will inform the Board's decision on next steps.

Recommendation 17.1 recommends that ICANN org create a framework to characterize the nature and frequency of name collisions and resulting concerns. The community inputs that the Board considered when acting on this recommendation showed that while some community groups are in support of the recommendation, others express concerns. For example, RySG, IPC, and Article 19 express concerns that this recommendation overlaps with or is in contradiction to the ongoing work related to Name Collision. Article 19 encourages revising the recommendation "so that it is not in contradiction with the recommendations outlined under the GNSO New Subsequent Procedures Draft Final Report" and "to note that measuring name collisions should be carried out under the ongoing framework pending full completion of the work carried out by the NCAP studies group".

The Board notes that Recommendation 17.1 has dependencies on the SSAC NCAP. The output of the NCAP studies will inform the Board's decision on next steps. The Board noted such overlap in its comments on the SSR2 Review Team draft report, and encouraged the SSR2 Review Team to consider how its recommendations may be consolidated into or passed through to ongoing work.

Recommendations 18.1, 18.2 and 18.3 recommend that ICANN org create and maintain a public archive of digests or readouts from various networking and security research conferences. The community inputs that the Board considered when acting on these recommendations showed that while several community groups support these recommendations by way of their

overarching support for all recommendations in the SSR2 Review Team Final Report, RySG and RrSG express concerns. For example:

- RySG - "In much the same way that ICANN monitors and offers neutral summary reports on legislative developments and identifier technology issues, it is reasonable for ICANN to do so for other topics related specifically to ICANN's mission and scope. However, it is unclear how recommending that ICANN offer an interpretation or analysis (including proposing additional studies) of these third-party efforts by specifically targeting only one part of the ICANN community is within either the Review Team's scope of work or ICANN's."
- RrSG - "Contract negotiations are between contracted parties and ICANN as detailed in the RAA and RA, and are not subject to public discussion and feedback from the ICANN community, including recommendations from peer-reviewed literature", and "it is not clear how the studies will be paid for, and how confirming peer-reviewed studies are beneficial or within ICANN's remit."

The Board notes that ICANN org currently already publishes reports of emerging technologies that are relevant to ICANN org's mission through its Office of the Chief Technology Officer (OCTO) publication series, and regularly provides updates the community, for example via recent Emerging Identifier Technology sessions at ICANN58, ICANN60, ICANN64, and ICANN66.

As the Board noted in its comment on the SSR2 Review Team draft report, the Board supports the work of OCTO and its determination of the needs for data and analysis to inform its work, and the Board is not clear about the value to the community of a potentially large-scale and costly effort associated with the implementation of this recommendation. While the Board agrees that there is merit to ICANN org performing an evaluation to ensure that it is tracking at an appropriate level to the work that ICANN does, the Board notes that many academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these

materials. In this manner, Recommendations 18.1 - 18.3 imply unbounded work. The Board would like to better understand the community's views as to if ICANN org should expend additional resources on this activity, in light of current existing work.

The Board directs the ICANN President and CEO, or his designee(s), to perform an evaluation of its tracking efforts already underway and provide this to the Board to ensure that ICANN org is tracking at an appropriate level to the work that ICANN does. Further, the Board directs the ICANN President and CEO, or his designee(s) to engage the community to understand if ICANN org should expend additional resources on this activity, in light of current existing work. This information will inform the Board's decision on next steps.

Recommendation 20.1 relates to establishing a formal procedure to specify the details of future key rollovers. No community groups express concerns about this recommendation. The Board expects that this recommendation would require significant resources to implement, while the cost versus benefit is not clear. Further, the Board notes that this recommendation has dependencies on research work that has not yet been conducted, such as algorithm rolls. The Board notes that alternative solutions, such as a process that contains evaluation checkpoints that allow circumstances to be evaluated and provide for potential course correction, may be more appropriate. In light of these considerations, the Board requires further information, including from community engagement as appropriate, in order to take dispositive action on this recommendation. The Board directs the ICANN President and CEO, or his designee(s) to gather further information, including via community engagement and engagement with the SSR2 Implementation Shepherds as appropriate on this recommendation. This information will inform the Board's decision on next steps.

SSR2 Recommendation 24.1 asks ICANN org to perform annual end-to-end testing of the full EBERO process with public documentation for the outcome. No community groups express concerns about this recommendation. The Board notes that some elements of this recommendation are not clear. For example, it is not clear if the SSR2 Review Team's intent is

for ICANN org conduct EBERO testing on "live" gTLDs with registrations. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendations that the Board determines to be pending, likely to be rejected unless additional information shows implementation is feasible.

The Board places six recommendations into "pending, likely to be rejected unless additional information shows implementation is feasible": 6.1, 6.2, 7.4, 9.2, 16.2 and 16.3. As specified in the Scorecard, the Board expects specific actions to take place in order to take further Board decision on these recommendations. The Board uses this category to communicate to the ICANN community that based on the information available to date, the Board anticipates that each of these recommendations will be rejected.

Recommendations 6.1 and 6.2 pertain to SSR vulnerability disclosures, including imposing additional requirements on contracted parties. The community inputs that the Board considered when acting on Recommendations 6.1 and 6.2 showed that while several commenters support the recommendations, others express concerns. RySG, Namecheap, and RrSG believe elements of the recommendations contemplate that ICANN org should unilaterally make modifications to the Registrar Accreditation Agreement (RAA). For example:

- RySG - "While the RySG supports its members adopting vulnerability disclosure policies as good business practice, it does not support ICANN acting as a clearinghouse, gatekeeper, or regulator of vulnerability disclosure policies
- Namecheap - "Namecheap does not support any of the components of the SSR2 Final Report that contemplate any modification of the RAA (including but not limited to Recommendations 6 and 8), and urges the ICANN Board to completely reject any of these recommendations."

- RrSG - "It is not the role of ICANN or the ICANN community to dictate the operational obligations of contractual parties especially without the participation, agreement, and approval of the contracted parties."

While IPC is supportive of these recommendations, IPC expresses a concern that "requir[ing] dotBrands to disclose all vulnerabilities in their business to ICANN...goes beyond ICANN's remit. At a minimum, any vulnerabilities should be limited only to those systems directly related to the operation of the TLD."

With regard to Recommendation 6.1, the Board notes that several elements of the recommendation are not clear. For example, as written, it is not clear how ICANN org should implement the recommendation in the event that there is not voluntary adoption, and may require a GNSO Policy Development Process. Possibly, the SSR2 Review Team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and Memorandums of Understanding". If this is the intent, while the Board supports contracted parties using best practices that align with the goals and objectives outlined in ICANN's Strategic Plan, making implementation of best practices mandatory would be a policy matter and not something ICANN org or Board can unilaterally impose in "contracts, agreements, and MOUs." Other elements of this recommendation that require clarification include, for example, how should SSR best practices/objectives be identified? How should ICANN org measure adoption? What is the threshold to evaluate ICANN org's promotional efforts as insufficient? The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

With regard to Recommendation 6.2, the Board notes there are three components of this recommendation, which each have different considerations. While ICANN org already does some of the things called for within the recommendation as ICANN org noted in its comments

on the SSR2 Review Team draft report, the recommendation's focus on disclosure appears difficult or nearly impossible to implement. The Board directs the ICANN President and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation and the possible process to implement it with the relevant parties. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendation 7.4 asks ICANN org to "establish a new site for [Disaster Recovery] for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories." The community inputs that the Board considered when acting on Recommendation 7.4 showed that, in general, commenters support the recommendation. However, RrSG notes "although the RrSG is generally supportive of this recommendation, it will defer to IANA regarding whether or not to create and maintain a KSK ceremony location outside of the United States."

The Board does not have enough information to consider resource implications of implementing this recommendation versus the expected benefit. The Board notes that in its comment on the SSR2 Review Team draft report, ICANN org asked the SSR2 Review Team to provide clear justification as to why it believes the benefits of a third disaster recovery site justifies the costs of such a site. While the recommendation states that the new site could replace "either the Los Angeles or Culpeper sites", the requested cost/benefit information is not provided in the SSR2 Review Team Final Report. Further, the Board notes Section 4.2 of the IANA Naming Function Contract[13] that prohibits IANA operations outside of the United States, and as such, the Board understands that implementation of this recommendation as written is not currently feasible for some portions of the IANA functions. These restrictions could be removed through contract amendments if there were a desire to do so from the ICANN community, which would require

[13] IANA Naming Function Contract (30 September 2016) Section 4.2 U.S. Presence: https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16

community consultation and discussion. The Board directs the ICANN President and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand elements of this recommendation that are not feasible as written, or are not clear, including if the SSR2 Review Team considered the benefit versus cost considerations. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps, which may include wider community consultation.

Recommendation 9.2 recommends ICANN org "proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data." The Board notes that ICANN org does not have authority to require validation beyond what is in the Registry Agreement and Registrar Accreditation Agreement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, including the authority the SSR2 Review Team understood that ICANN org's Contractual Compliance team has to carry out the recommended actions. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Recommendations 16.2 and 16.3 relate to privacy requirements around the Registration Directory Service (RDS). The community inputs that the Board considered when acting on Recommendations 16.2 and 16.3 showed that while several community groups support the recommendations, RySG and RrSG express some concerns that these recommendations do not address a specific problem statement. Concerns in particular with regard to recommendation 16.3 include, for example:

- RySG - "16.3 suggests that ICANN Compliance should audit Registry and Registrar compliance with a Registry or Registrar's own internal policies and procedures as opposed to its contractual obligations with ICANN. Such a recommendation exceeds the scope of ICANN Compliance's role to enforce contractual requirements."

- RrSG - "This is outside of ICANN's scope. ICANN is not a DPA, and the audit would need to cover a number of countries and jurisdictions around the world, and it is unclear how ICANN has the expertise or resources to conduct such an audit."

With regard to Recommendation 16.2, the Board is not clear as to what is meant by "facilitate law enforcement needs" and how that is relevant to the role of ICANN org's Contractual Compliance team. As written, ICANN org does not have the authority to do this. Further, the intent of the recommendation is not clear, specifically why the SSR2 Review Team understands the existing subject matter experts and Chief Data Protection Officer roles within ICANN org are inadequate to achieve the requirements of this recommendation. The Board understands that ICANN org's Contractual Compliance team has subject matter experts in the areas listed to the extent that they are necessary for contract enforcement. For other matters and as necessary, ICANN org's Contractual Compliance members can refer to ICANN org's Chief Data Protection Officer for guidance regarding the specific areas listed. Through the Contractual Compliance team, ICANN org enforces policies that have been adopted by the community and makes operational and structural changes as needed to carry out its enforcement role. The Board directs the ICANN President and CEO, or his designee(s), to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, as well as other elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Further, with regard to Recommendation 16.3 which recommends for ICANN org to "conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches"; as the Board noted in its comment on the SSR2 Review Team draft report, ICANN org does not specifically require registrars to have "privacy policies." ICANN org's Contractual Compliance team cannot audit something that is not an ICANN contractual requirement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand the SSR2

Review Team's intent of the recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Which stakeholders or others were consulted?

As required by ICANN's Bylaws, the SSR2 Review Team sought community input on its draft report through a Public Comment proceeding opened in January 2020. A total of 18 community submissions were posted to the forum. Additionally, the SSR2 Review Team conducted engagement sessions at ICANN58, ICANN60, ICANN63, ICANN64, and ICANN69, and community webinars on its draft and final reports in February 2020 and February 2021 respectively. The SSR2 Review Team summarized its approach to how Public Comments and inputs received were considered in Appendix H of its final report.

ICANN's Bylaws call for the final report to be posted for Public Comment to inform Board action on final recommendations. The Public Comment proceeding on the SSR2 Review Team Final Report opened on 28 January 2021 and closed on 8 April 2021. 19 submissions were posted to the forum. The Board considered the public comment submissions during its assessment of the final recommendations, as noted within the rationale supporting the Board action on each recommendation.

In addition to consulting with the SSR2 Review Team throughout the duration of the review, the Board provided a public comment on the SSR2 Review Team draft report, as did ICANN org. In its comment, the Board noted that: "Input from the Board is intended to contribute to the refinement of the recommendations and address areas that may benefit from clarification. The Board has general observations on several topics, including: the formulation and prioritization of the draft recommendations; draft recommendations that are outside of the Board's oversight responsibilities; draft recommendations that overlap with other work ongoing in the community", among other things. ICANN org's comment focused on the operational elements of the SSR2 Review Team draft report on which ICANN org sought clarification and areas that ICANN org felt could benefit from refinement to ensure the SSR2 Review Team produced effective

recommendations. ICANN org's comment addressed "formulation of draft recommendations, feasibility of implementation of draft recommendations, recommendations that ICANN org considers to be implemented already." Additionally, ICANN org requested clarification of certain terms, noting that "[a] number of SSR2 RT recommendations include specific terms that ICANN org may not fully understand in the context of the SSR2 recommendation. To ensure that the identified issues or risks, the recommended solutions, and the expected impact of implementation of the recommendation are clearly defined and understood by all, ICANN org encourages the SSR2 RT to define" various terms, for example: "SSR-related best practices." In most cases, the SSR2 Review Team did not address or respond to the observations and questions identified by the Board and ICANN org in their respective comments. As noted above in the rationale section for specific recommendations, because the previously noted observations and questions had not been addressed, the Board and ICANN org will seek clarity from the SSR2 Implementation Shepherds, within bounds of their current role to provide clarity.

The Board has also engaged with the SSR2 Implementation Shepherds, to provide an update on the Board's work since the SSR2 Review Team Final Report was published and to apprise the SSR2 Implementation Shepherds of the categorization approach. The SSR2 Implementation Shepherds underscored the importance of understanding how the various pending recommendations map to other work where there are dependencies and what the triggers will be for the Board to be able to take dispositive action at a later date. The Board reviewed next steps, setting clear expectations of further engagement after the Board action, in order to seek clarity on the SSR2 Review Team's intent and aspects of recommendations that are not clear.

What concerns or issues were raised by the community?

Public Comments highlight that there is a broad and diverse range of community viewpoints across a number of elements of the SSR2 Review Team Final Report.

RySG, PIR, Tucows, Namecheap, and RrSG express concerns that some recommendations are contrary to ICANN's multistakeholder model, for example recommending that ICANN org make unilateral changes to the Registry Agreement, or initiate a Policy Development Process.

RySG, PIR, i2Coalition, Namecheap, and RrSG express concerns that some recommendations repeat or significantly overlap with ongoing work. For example, with recommendations from the CCT Review Team, with the NCAP, or with functions that ICANN org already provides.

Tucows, Namecheap, and RrSG express concerns that the SSR2 Review Team did not include representation from contracted parties, and that public input from these groups was not adequately considered. As such, these groups believe that some of the final recommendations are unbalanced and biased.

The above noted concerns and issues, along with specific concerns on individual recommendations are incorporated into the rationale section for each recommendation and addressed therein.

Are there positive or negative community impacts?

Taking action on the SSR2 recommendations will contribute to ensuring ICANN meets its commitments relative to the Bylaws-mandated reviews and the role they play in ICANN's accountability and transparency, as well as enhancing the security, stability, and resiliency of the DNS. Additionally, the Board action on the recommendations will have a positive impact on the continuous improvement of ICANN as a whole.

Approved recommendations are consistent with ICANN's Mission and serve the public interest. The Board acknowledges that approving recommendations that duplicate or significantly overlap with existing ICANN org operations, or would require the Board or ICANN org to act outside of the remit could have negative community impacts. The Board considered the potential negative community impacts as part of its action. Additional impacts resulting from further actions on recommendations will be assessed at that time.

The Board notes important lessons learned from this review, which in part informed recommendations from the Third Accountability and Transparency Review Team (ATRT3) on

improving future reviews. These lessons will be considered by ICANN org, Board, and community as they look at ways to enhance effectiveness of reviews and their outcomes.

What significant materials did the Board review?

The Board reviewed various significant materials and documents as part of its consideration of the SSR2 recommendations. These included the SSR2 Draft Report for Public Comment, the Report of Public Comments on the SSR2 Draft Report, the SSR2 Review Team Final Report, the Report of Public Comments on the Final Report, and the ICANN org assessment of SSR2 recommendations. The Board, with the support of ICANN org, reviewed the recommendations as drafted by the SSR2 Review Team as well as the proposed measures of success in order to assess feasibility.

Are there fiscal impacts or ramifications on ICANN (strategic plan, operating plan, budget); the community; and/or the public?

For the group of recommendations that the Board approved, the implementation is subject to prioritization, risk assessment and mitigation, costing and implementation considerations, which will provide a further view of the fiscal impact. It is expected that any recommendations that require incremental resources should be included into operational planning and budgeting processes, allowing for appropriate community consideration and prioritization, as applicable, of planned work.

Implementation of approved recommendations may impact ICANN org and community bandwidth and resources. For the recommendations the Board is placing in "pending", the Board expects specific actions to take place in order to take further Board decision on these recommendations, which in some cases will require time from the community to provide input. In particular, the Board recognizes the workload of the SSR2 Implementation Shepherds will increase.

Are there any security, stability or resiliency issues relating to the DNS?

By nature of the SSR2 Review, implementation of the recommendations may impact how ICANN meets its security, stability, stability, and resiliency commitments. The Board considered this potential impact as part of its deliberations. Approved recommendations are consistent with ICANN's Mission, serve the public interest, and fall within the Board's remit.

Is this action within ICANN's Mission? How does it relate to the global public interest?

This action is within ICANN's Mission and mandate and in the public interest as it is a fulfillment of an ICANN Bylaw, as articulated in Section 4.6. ICANN's reviews are an important and essential part of how ICANN upholds its commitments.

Is this either a defined policy process within ICANN's Supporting Organizations or ICANN's Organizational Administrative Function decision requiring Public Comment or not requiring Public Comment?

Public Comments were received prior to Board consideration.

Signature Block:

Submitted by: Theresa Swinehart

Position: Senior Vice President

Date Noted: 22 July 2021

Email: theresa.swinehart@icann.org

ICANN Org Assessment: SSR2 Recommendations

- SSR2 Final Report: https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf
- Report of Public Comments (Final Report): https://www.icann.org/en/system/files/files/report-comments-ssr2-final-report-10may21-en.pdf
- Report of Public Comments (Draft Report): https://www.icann.org/en/system/files/files/report-comments-ssr2-rt-draft-report-22apr20-en.pdf

RECOMMENDATIONS SUMMARY TABLE & FUNCTION LEADS

#	Recommendation	SSR2 assigned owner	SSR2 assigned priority	Relevant report section (link)	Function to lead analysis
Section C: SSR1 Implementation & Intended Effects					
SSR2 Recommendation 1: Further Review of SSR1					
1.1	The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 Recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations).	ICANN Board and ICANN org	Low	Section C: SSR1 Review	Implementation ops
Section D: Key Stability Issues within ICANN (Recs 2 - 7)					
SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management					
2.1	ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions.	ICANN org	Medium - High	Section D1: Organization Structure Improvements - C Suite Security Position	OCTO / E&IT
2.2	ICANN org should include as part of this role's description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that	ICANN org	Medium - High	Section D1: Organization Structure Improvements - C Suite	OCTO / E&IT

	impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position.			Security Position	
2.3	ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach.	ICANN org	Medium - High	Section D1: Organization Structure Improvements - C Suite Security Position	OCTO / E&IT
2.4	ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, supply chains for hardware and software, and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual	ICANN org	Medium - High	Section D1: Organization Structure Improvements - C Suite Security Position	OCTO / E&IT

	terms.				
SSR2 Recommendation 3: Improve SSR-Related Budget Transparency					
3.1	The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually.	ICANN org	High	Section D2: SSR-Related Budgets & Reporting	OCTO / E&IT
3.2	The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN Strategic Plan goals and objectives. ICANN org should implement those mechanisms through a consistent, detailed, annual budgeting and reporting process.	ICANN Board and ICANN org	High	Section D2: SSR-Related Budgets & Reporting	Finance
3.3	The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle.	ICANN Board and ICANN org	High	Section D2: SSR-Related Budgets & Reporting	Finance
SSR2 Recommendation 4: Improve Risk Management Processes and Procedures					
4.1	ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them.	ICANN org	High	Section D3: Risk & Security Management	Risk mgmt.

4.2	ICANN org should adopt and implement ISO 31000 “Risk Management” and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures).	ICANN org	High	Section D3: Risk & Security Management	Risk mgmt.
4.3	ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org’s activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications).	ICANN org	High	Section D3: Risk & Security Management	Risk mgmt.
SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications					
5.1	ICANN org should implement an ISMS and be audited and certified by a third party along the lines of	ICANN org	High	Section D3: Risk & Security Management	E&IT

	industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement.				
5.2	Based on the ISMS, ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies.	ICANN org	High	Section D3: Risk & Security Management	E&IT
5.3	ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers.	ICANN org	High	Section D3: Risk & Security Management	E&IT
5.4	ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes to manage risk, security, and vulnerabilities.	ICANN org	High	Section D3: Risk & Security Management	E&IT
SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency					
6.1	ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the	ICANN org	High	Section D3: Risk & Security Management	OCTO

	contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs.				
6.2	ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.	ICANN org	High	Section D3: Risk & Security Management	GDS
SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures					
7.1	ICANN org should establish a Business Continuity Plan for all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.	ICANN org	Medium - High	Section D4: Business Continuity Management & Disaster Recovery Planning	E&IT
7.2	ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server	ICANN org	Medium - High	Section D4: Business Continuity Management & Disaster Recovery Planning	IANA

	System Advisory Committee (RSSAC) and the Root Server Operators (RSO).				
7.3	ICANN org should also establish a DR Plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031.	ICANN org	Medium - High	Section D4: Business Continuity Management & Disaster Recovery Planning	E&IT
7.4	ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org.	ICANN org	Medium - High	Section D4: Business Continuity Management & Disaster Recovery Planning	E&IT
7.5	ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans.	ICANN org	Medium - High	Section D4: Business Continuity Management & Disaster Recovery Planning	E&IT
Section E: Contracts, Compliance, and Transparency around DNS Abuse (Recs 8 - 16)					
SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties					

8.1	ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the domain name system for end-users, businesses, and governments.	ICANN org	Medium	Section E1: Unachieved Safeguards for the New gTLD Program	GDS
SSR2 Recommendation 9: Monitor and Enforce Compliance					
9.1	The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse related obligations in contracts, baseline agreements, temporary specifications, and community policies.	ICANN Board	High	Section E1: Unachieved Safeguards for the New gTLD Program	Compliance
9.2	ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org.	ICANN org	High	Section E1: Unachieved Safeguards for the New gTLD Program	Compliance
9.3	ICANN org should have compliance activities audited externally at least annually and publish the audit	ICANN org	High	Section E1: Unachieved Safeguards for	Compliance

	reports and ICANN org response to audit recommendations, including implementation plans.			the New gTLD Program	
9.4	ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.	ICANN org	High	Section E1: Unachieved Safeguards for the New gTLD Program	Compliance
SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms					
10.1	ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct—ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication.	ICANN org	High	Section E2: Challenges: Definitions and Data Access	Policy / Gutsy Star
10.2	Establish a staff-supported,	ICANN	High	Section E2:	Policy / Gutsy

	cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.	org		Challenges: Definitions and Data Access	Star
10.3	Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page.	ICANN org	High	Section E2: Challenges: Definitions and Data Access	Comms
SSR2 Recommendation 11: Resolve CZDS Data Access Problems					
11.1	The ICANN community and ICANN org should take steps to ensure that access to CZDS data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials.	ICANN community and ICANN org	Medium	Section E2: Challenges: Definitions and Data Access	GDS
SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review					
12.1	ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities.	ICANN org	Medium	Section E2: Challenges: Definitions and Data Access	OCTO

12.2	ICANN org should structure its agreements with data providers to allow further sharing of the data for non-commercial use, specifically for validation or peer-reviewed scientific research. This special no-fee non-commercial license to use the data may involve a time-delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN web site. ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting.	ICANN org	Medium	Section E2: Challenges: Definitions and Data Access	OCTO
12.3	ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports.	ICANN org	Medium	Section E2: Challenges: Definitions and Data Access	OCTO
12.4	ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS.	ICANN org	Medium	Section E2: Challenges: Definitions and Data Access	GDS
SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting					
13.1	ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only	ICANN org	High	Section E2: Challenges: Definitions and Data Access	GDS/E&IT

	summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all gTLDs; the participation of each ccTLD would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.				
13.2	ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS	ICANN org	High	Section E2: Challenges: Definitions and Data Access	Compliance
SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements					
14.1	ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold.	ICANN org	High	Section E3: PDP Alternatives	Legal / Policy
14.2	To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains.	ICANN org	High	Section E3: PDP Alternatives	GDS
14.3	Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and then issue a notice to the relevant party.	ICANN org	High	Section E3: PDP Alternatives	Compliance

14.4	ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Compliance should move to the de-accreditation process.	ICANN org	High	Section E3: PDP Alternatives	Compliance
14.5	ICANN org should consider offering financial incentives: contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold.	ICANN org	High	Section E3: PDP Alternatives	GDS
SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements					
15.1	After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported EPDP to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template.	ICANN org	High	Section E3: PDP Alternatives	Policy
15.2	The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse	ICANN org	High	Section E3: PDP Alternatives	Policy

	report/response report timelines, and ICANN Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days.				
SSR2 Recommendation 16: Privacy Requirements and RDS					
16.1	ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the RDS.	ICANN org	Medium	Section E4: Privacy & Data Stewardship	Comms
16.2	ICANN org should create specialized groups within the contract compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems).	ICANN org	Medium	Section E4: Privacy & Data Stewardship	Compliance
16.3	ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in	ICANN org	Medium	Section E4: Privacy & Data Stewardship	Compliance

	place to address privacy breaches.				
Section F: Additional SSR Related Concerns Regarding the Global DNS (Recs 17 - 24)					
SSR2 Recommendation 17: Measuring Name Collisions					
17.1	ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which Controlled Interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the appropriate handling of sensitive data and security threats.	ICANN org	Medium	Section F1: Name Collision	OCTO
17.2	The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion.	ICANN community and ICANN org	Medium	Section F1: Name Collision	Policy
SSR2 Recommendation 18: Informing Policy Debates					
18.1	ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the	ICANN org	Low	Section F2: Research & Briefings	OCTO

	ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior.				
18.2	ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature.	ICANN org	Low	Section F2: Research & Briefings	OCTO
18.3	ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS.	ICANN org	Low	Section F2: Research & Briefings	OCTO
SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite					
19.1	ICANN org should complete the development of a suite for DNS resolver behavior testing.	ICANN org	Low	Section F3: DNS Testbed	OCTO
19.2	ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained.	ICANN org	Low	Section F3: DNS Testbed	OCTO
SSR2 Recommendation 20: Formal Procedures for Key Rollovers					
20.1	ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points,	ICANN org	Medium	Section F4: Root Zone Registry Concerns	IANA

	exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for public comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process.				
20.2	ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root KSK rollover process.	ICANN org	Medium	Section F4: Root Zone Registry Concerns	IANA
SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators					
21.1	ICANN org and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email.	ICANN org and PTI	Medium	Section F4: Root Zone Registry Concerns	IANA
SSR2 Recommendation 22: Service Measurements					
22.1	For each service that ICANN org has authoritative purview over, including root-zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational	ICANN org	Low	Section F4: Root Zone Registry Concerns	E&IT

	status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and metrics on a single page on the icann.org web site, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior).				
22.2	ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility.	ICANN org	Low	Section F4: Root Zone Registry Concerns	E&IT
SSR2 Recommendation 23: Algorithm Rollover					
23.1	PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS.	PTI	Medium	Section F4: Root Zone Registry Concerns	IANA
23.2	As a root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking	PTI	Medium	Section F4: Root Zone Registry Concerns	IANA

	into consideration the lessons learned from the first root KSK rollover in 2018.				
SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process					
24.1	ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised, and publish the results.	ICANN org	Medium	Section F5: Emergency Back-end Registry Operator (EBERO)	GDS
24.2	ICANN org should make the Common Transition Process Manual easier to find by providing links on the EBERO website.	ICANN org	Medium	Section F5: Emergency Back-end Registry Operator (EBERO)	GDS

ICANN ORG'S APPROACH: ANALYSIS AND ASSESSMENT TO INFORM BOARD ACTION

Introduction

Purpose

The purpose of this document is to aggregate ICANN org's analysis, assessments and considerations to inform Board action on SSR2 recommendations. The document includes explanation of the approach and the detailed information pertaining to each recommendation that the Board reviewed and considered in arriving at their decision. Key considerations from this assessment are summarized in the Scorecard, and serve as the basis for the rationale supporting the Board's decision.

Big-picture approach

As discussed during the Board workshop, the SSR2 Review is important, mandated by the ICANN Bylaws and relating to key elements of ICANN's Strategic Plan. The proposed categorization factors in dependencies to the SSR2 recommendations relating to these areas, including community provided Advice, Policy or other community recommendations that relate to security, stability, and resiliency, a topic of strategic importance and one that is essential to carrying out the Mission of ICANN. SSR2 recommendations are considerable in number (63 recommendations), cannot be addressed in silos, and many are complex and touch on other significant areas of work underway - for example, DNS Security Threats/DNS Abuse, Sub-Pro, Name Collision.

With 63 SSR2 recommendations to consider, the categorization and approach will allow for sufficient time for fulsome analysis and consideration of the relevant significant factors, including the diverse opinions registered through public comment and other input. At the same time, the categorization allows for community communications and transparency in assessing the approach to the recommendations, while ensuring Board accountability to the Bylaws-mandated deadline to take action on the recommendations by 25 July 2021.

Systematic Approach - categorization

Noting some broad areas and themes in relation to the SSR2 recommendations, many of which are emphasised in public comments, the Board developed six categories of Board action on SSR2 recommendations to move some recommendations to final action now, while allowing for sufficient additional time for fulsome analysis and consideration of the relevant significant factors impacting the feasibility of implementing other recommendations. The categories include:

- Recommendations the Board approves, subject to prioritization, risk assessment and mitigation, costing and implementation considerations; and recommendations that the Board approves, with the understanding that they are already fully implemented. Approved recommendations are consistent with ICANN's Mission, serve the public interest, and fall within the Board's remit. Further, approved recommendations are clear, do not have

dependencies (including any requiring mitigation of other work), have community support and a clear path to implementation.

- Recommendations the Board rejects because the recommendation cannot be approved in full. The Board notes that, while some portions of the recommendation could be feasible, and in some cases work is already underway, there are limitations imposed by other portions of the same recommendation that could impact feasibility. While the Board agrees in principle with the intent of many of these recommendations, the Board does not have the option of selectively approving some parts and rejecting other parts of a single, undivisible community recommendation and must act on a recommendation as written and not as interpreted by ICANN org or the Board.
- Recommendations the Board rejects.
- Recommendations that the Board determines to be pending, likely to be approved once further information is gathered to enable approval. The Board expects specific actions to take place in order to take further Board decision on these recommendations, and uses this category to communicate to the ICANN community that based on the information available to date, the Board anticipates that each of these recommendations will be approved.
- Recommendations that the Board determines to be pending, holding to seek clarity or further information. The Board is unable to signal at this time whether it is likely to accept or reject each of these recommendations pending the collection of additional information.
- Recommendations that the Board determines to be pending, likely to be rejected unless additional information shows implementation is feasible. The Board expects specific actions to take place in order to take further Board decision on these recommendations. The Board uses this category to communicate to the ICANN community that based on the information available to date, the Board anticipates that each of these recommendations will be rejected.

Next steps

The recommendations that the Board will approve by 25 July - these recommendations will be approved subject to prioritization, risk assessment and mitigation, costing and implementation considerations. An implementation plan will be developed, including resource needs and scheduling considerations, to inform the timing of implementation. To the extent implementation planning will require clarifications from the SSR2 Implementation Shepherds, ICANN org will engage with the to seek clarification. ICANN org will provide periodic status updates on the progress of implementation work to the Board and the community.

Some recommendations that the Board will approve by 25 July call for actions that have already been implemented by ICANN org. Based on the supplied evidence of this, there will be no further action required from ICANN org and the implementation of these recommendations will be considered complete.

For recommendations that the Board will place into the pending categories, the Board will commit to take further action on these recommendations subsequent to the completion of intermediate steps as identified in the Scorecard. At Board's direction, ICANN org will provide to the Board relevant information, as requested in the Scorecard, and advise if additional time is needed within six months from this Board action.

Themes and overarching considerations

ICANN org reviewed the recommendations as drafted by the SSR2 Review Team as well as the proposed measures of success in order to assess feasibility. At times, ICANN org identified that while some portions of a recommendation could be feasible, there were limitations imposed by the other portions of the same recommendation that could impact feasibility. ICANN org still identified all efforts that it understood as supporting the broader intent of each recommendation.

SSR2 recommendations are considerable in number, complex, and have interdependencies with other significant areas of work underway.
The SSR2 Review Team organized 63 distinct recommendations into 24 groups, with one single recommendation on the implementation of SSR1 recommendations comprising 28 underlying recommendations. The Board notes that 23 recommendations issued by the SSR2 Review Team relate to DNS security threats/DNS abuse, while others also relate to other significant areas of work underway within ICANN, such as New gTLD Subsequent Procedures and Name Collision.

Some recommendations contain components that the Board cannot approve, along with components that are feasible, and in some cases already being done.
ICANN org reviewed the recommendations as drafted by the SSR2 Review Team as well as the proposed measures of success in order to assess feasibility. At times, while some portions of a recommendation could be feasible, there are limitations imposed by the other portions of the same recommendation that could impact feasibility.

ICANN org notes the community intent in incorporating Specific Reviews into the ICANN Bylaws in 2016 was for the Board not to have the option of selectively approving some parts and rejecting other parts of a community recommendation. Similarly, the community intent was to have the Board act on a recommendation as written, not as interpreted by ICANN org or Board. Thus, the assessment of the extent to which prior review recommendations have been implemented and the extent to which the implementation of such recommendations has resulted in the intended effect is left to the next community-led review team, based on implementation report provided by ICANN org and the SSR2-defined measures of success.

ICANN org further notes that the Board may wish to direct action from ICANN org on some of the ideas within the recommendations. In those cases, such actions would not be tracked as part of the tracking of the implementation of SSR2 recommendations.

Some recommendations are polarizing, with public comments reflecting different, often opposing views.
Recent advice and public input on SSR topics further suggest that the Board and org should ensure full analysis and consideration, and where needed, additional community consultation, of inconsistencies with advice or other community work and public input. Implementation of any recommendations should complement existing advice, Board-accepted recommendations, public input, and should align with ICANN's role in security, stability, and resiliency.

Several recommendations repeat or duplicate or significantly overlap with existing ICANN org operations, or recommendations issued by other Specific Review team.
The gTLD Registries Stakeholder Group (RySG), Public Interest Registry (PIR), i2Coalition, Namecheap, and the Registrar Stakeholder Group (RrSG) express concerns that some recommendations repeat or significantly overlap with ongoing work, including ICANN org work,

cross-community work, policy processes such as the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team, and recommendations from other review teams including the Competition, Consumer Trust, and Consumer Choice (CCT) Review Team. Noting the public input on recommendations that duplicate or significantly overlap with existing ICANN org operations, or recommendations issued by other Specific Review teams, the Board is taking the action of placing many of these recommendations into a pending category, directing ICANN org to complete the intermediate steps that would support in eventually accepting or rejecting each recommendation. These intermediate steps include seeking clarification from the SSR2 Implementation Shepherds, consulting with the ICANN community or monitoring developments of activities that are dependencies.

Some recommendations contemplate that the ICANN Board or ICANN org should unilaterally develop policy outside of the GNSO Council's Policy Development Process.
Some commenters note concerns that some SSR2 recommendations as written do not respect the Bylaws-mandated policy development roles within the multistakeholder model. RySG, PIR, Tucows, Namecheap, and RrSG all note that they do not support recommendations that contemplate modifications to the Registry Agreement (RA) or the Registrar Accreditation Agreement (RAA) outside of the defined Policy Development Process (PDP) or contract negotiations process. The Board and ICANN org take in the inputs of the community and strive to carefully reflect those inputs in the decisions made with ICANN org and Board, as an essential part of serving the public interest. The Board may wish to encourage ICANN to continue bilateral discussions with the contracted parties in a way that enhances the security, stability, and resiliency of the DNS and to strive to have these bilateral discussions be transparent to the general public, in order to continue building trust.

Some recommendations do not clearly address a fact-based problem, or articulate what cost/benefit would be derived or how the desired outcome envisioned by the Review Team would add value and improve security, stability, and resiliency.
RySG, Namecheap, and RrSG note this as a concern in their public comments on the SSR2 Review Team Final Report.

In its comment on the SSR2 Review Team draft report, the Board noted that "it is helpful for the Board to have an understanding of the particular issues or risks that each recommendation intends to address...Clear articulation of the observed issue gives insight into the intent of the recommendation and the justification for why it should be adopted. With this in mind, the Board notes that a number of the SSR2 RT's recommendations, as currently drafted, do not clearly define the identified issues or risks, the rationale for the recommended solutions, the expected impact of implementation, or what relevant metrics could be applied to assess implementation." ICANN org reiterated these points in its comment on the SSR2 Review Team draft report. Throughout the review process, the Board and ICANN org also encouraged the SSR2 Review Team to consider the Operating Standards for Specific Reviews and the guidance within on how to formulate concrete fact-based problem statements.

In many cases where recommendations do not clearly address a fact-based problem, or articulate what cost/benefit would be derived or how the desired outcome envisioned by the Review Team would add value and improve security, stability, and resiliency, the Board may wish to place the recommendations into a pending category, directing ICANN org to complete the intermediate steps that would support in eventually accepting or rejecting each recommendation. These intermediate

steps may include seeking clarification from the SSR2 Implementation Shepherds, for example on what the SSR2 Review Team's intended the recommendation would mitigate, or facts that led the SSR2 Review Team to believe that the benefit would justify the cost.

There are significant interdependencies of the SSR2 recommendations with other community work, including recent advice and public input. For example:

- GNSO New gTLD Subsequent Procedures Final Outputs for ICANN Board Consideration (Public Comment 22 April - 1 June 2021
    - Includes several elements related to security, stability, and resiliency (Topic 26 - p. 118)
- ALAC Advice to the ICANN Board on Subsequent Procedures (16 April 2021)
    - Includes advice relating to CCT recs, DNS abuse mitigation, name collision.
- SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (19 March 2021
    - SSAC proposes a general framework of best practices and processes to streamline reporting DNS abuse and abuse on the Internet in general.
    - SSAC provides an 'alternative view' to SSR2 rec 13.1 (Group 2)
- SAC116: SSAC Comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report (22 March 2021)
    - The report highlights some very critical issues for ICANN and the recommendations in the report illustrate some fundamental requirements for timely action to address these issues.
- GAC Communique ICANN70: CCT Review and Subsequent Rounds of New gTLDs (follow up on previous advice) (25 March 2021)
    - The GAC is seeking a coordinated approach on the implementation of the specified Recommendations from the CCT Review ahead of the potential launch of a new round of gTLDs.
    - A number of SSR2 recommendations pertaining to DNS abuse definitions overlap with CCT recommendations that are in 'Pending' status as the Board requires more information before it can take action (10.1 - 10.3, 12.4, 14.5 - All in Group 2/needs more work).
- SSAC Name Collision Analysis Project (NCAP)
    - In March 2021 the Board accepted NCAP Study 1 and directed NCAP Discussion Group to proceed with Study 2. Board affirmed the continued relevance of the nine questions related to name collisions presented in Board resolutions 2017.11.02.29 - 2017.11.02.31, especially questions (7) and (8) concerning criteria for identifying collision strings and determining if collision strings are safe to be delegated.

Recommendation 1: Further Review of SSR1

Recommendation 1.1	
Recommendation text:	The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 Recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations).
SSR2-defined measures of success:	n/a
Owner (SSR2 assigned):	ICANN Board and ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	Implementation ops
Summary of Public Comment:	Elements of support: ● Commenters expressed general support for this recommendation. ● Some commenters (RySG, i2Coalition) ask that the ICANN Board consider ongoing community work and identify areas of potential duplication or overlap when taking action on the recommendation. Elements of concern: ● Concerns on passage of time since 2012 & publication of the SSR1 Recommendations.
Dependencies:	None
Considerations:	The Board in it's assessment of these recommendations and possible approval should factor in that since the SSR1 recommendations, and the SSR2 finalization of these recommendations (which included multiple briefings by staff), much has changed with ICANN org's processes and procedures to address review recommendations and implementation. While the SSR1 recommendations are important, assuming none of them mitigate current matters, it may be prudent for ICANN org's resources to go towards implementation of SSR2 recommendations factoring in lessons learned from SSR1. ICANN org understands the importance of completing implementation work in line with community expectations and that lessons learned from the current cycle of specific reviews will inform future review work to enhance the effectiveness of review

	outcomes, in terms of implementable recommendations and timely and clearly presented status of implementation work. SSR1 recommendations were written at a time when ICANN was structured differently than today, and it may not be practical to go back and re-execute a plan to complete the SSR1 recommendations; there may be substantial differences of opinion within the ICANN community, Board and org on completion of the SSR1 recommendations. ICANN org also notes that SSR2's findings in the appendix (D) of its final report are to be considered by ICANN org as guidance in its review of the implementation of the SSR1 recommendations. The proposed approach is in line with the rationale for the similar recommendation from ATRT3 that the Board approved.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management

Recommendation 2.1	
Recommendation text:	ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management (2.1 - 2.4) This recommendation can be considered implemented when ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations. This recommendation can be considered effective when ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	
Lead:	OCTO / E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● BC and IPC make specific statements of support for this grouping of recommendations, pointing to the SSR2 Review Team's assessment of SSR1 implementation as indicative as a reason the new position is warranted. ● GAC believes "such a centralized role may have various benefits", however GAC notes it "would not wish to presume expertise in ICANN's internal administration of executive functions". ● RySG notes support for this grouping of recommendations "insofar as they represent strategic requirements for ICANN Org risk management", however, RySG does not support the creation of a new position. Afnic offers its full support to the RySG's comment

	Elements of concern: ● RySG, i2Coalition, Namecheap, and RrSG do not support creation of the new position called for in this grouping of recommendations. These commenters believe that the work specified in the role description is already being carried out by members of ICANN org, and it is not clear as to why the new position is needed in light of the existing work.
Dependencies:	None
Considerations:	Recommendations 2.1 - 2.4 should be treated as a group: In their respective public comments on the draft report, ICANN org and Board encouraged the SSR2 RT to provide specific details as to what issues or risks the SSR2 RT identified with the current operations, how the recommendation would address these, and what metrics could be applied to assess implementation. As noted in ICANN org's public comment on the SSR2 draft report, because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages), ICANN org made the conscious decision to distribute the various security functions to the relevant functional areas within the organization. These functional teams work closely not only with one another but also with the Risk Committee of the Board, which provides oversight as to the risk based functions for which ICANN org is responsible. The Board has the oversight role not the authority to organize the structures of the ICANN org, which is a key aspect within the role of the ICANN CEO and part of his accountability. ICANN org is in a relatively unique state in regards to security management. There is the traditional role of data and systems security that most organizations have and protect against as well as the security and well-being of its staff. However, since ICANN the org facilitates numerous meetings of scale with its communities and with its particular role in managing portions of the Internet's unique identifier systems as defined in its Bylaws, which are both different types of physical and data security, the ICANN org felt that the scope to be too big and the breadth too diverse to manage these distinctly different functions under one reporting structure. As the organization matured over the years, it became clear that these security related functions would be best managed in a distributed manner with specific and narrow responsibilities to be managed by the executive of the functional team best suited for the specified role. This decision was not made lightly and the org continues to evaluate and refine where these responsibilities lie. ICANN org made the decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN

	org is responsible. In addition, the org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. This body is therefore a mechanism that provides org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject

Recommendation 2.2	
Recommendation text:	ICANN org should include as part of this role's description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management (2.1 - 2.4) This recommendation can be considered implemented when ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations. This recommendation can be considered effective when ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high

ICANN org assessment:	
Lead:	OCTO / E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● BC and IPC make specific statements of support for this grouping of recommendations, pointing to the SSR2 Review Team's assessment of SSR1 implementation as indicative as a reason the new position is warranted. ● GAC believes "such a centralized role may have various benefits", however GAC notes it "would not wish to presume expertise in ICANN's internal administration of executive functions". ● RySG notes support for this grouping of recommendations "insofar as they represent strategic requirements for ICANN Org risk management", however, RySG does not support the creation of a new position. Afnic offers its full support to the RySG's comment Elements of concern: ● RySG, i2Coalition, Namecheap, and RrSG do not support creation of the new position called for in this grouping of recommendations. These commenters believe that the work specified in the role description is already being carried out by members of ICANN org, and it is not clear as to why the new position is needed in light of the existing work.
Dependencies:	Dependent on implementation of SSR2 recommendation 2.1.
Considerations:	Recommendations 2.1 - 2.4 should be treated as a group: It is not clear how this recommendation would improve current processes that are in place. In their respective public comments on the draft report, ICANN org and Board encouraged the SSR2 RT to provide specific details as to what issues or risks the SSR2 RT identified with the current operations, how the recommendation would address these, and what metrics could be applied to assess implementation. As noted in ICANN org's public comment on the SSR2 draft report, because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages), ICANN org made the conscious decision to distribute the various security functions to the relevant functional areas within the organization. These functional teams work closely not only with one another but also with the Risk Committee of the Board, which provides oversight as to the risk based functions for which ICANN org is responsible.

	The benefit to implementing the recommendation versus the risks and cost considerations is not clear. It is not clear what issues the review team intends the CSO/CISO role and reorganization will address and why the review team believes that the creation of the CSO/CISO role and reorganizing structures intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk/disruption to staff and cost. There may be benefits in increased periodic communication on SSR activities. This is already partially performed as part of the current annual planning process but could be enhanced consistently with the presumed intent of the recommendation 2.2. The Board has the oversight role not the authority to organize the structures of the ICANN org, which is a key aspect within the role of the ICANN CEO and part of his accountability. ICANN org is in a relatively unique state in regards to security management. There is the traditional role of data and systems security that most organizations have and protect against as well as the security and well-being of its staff. However, since ICANNthe org facilitates numerous meetings of scale with its communities and with its particular role in managing portions of the Internet's unique identifier systems as defined in its Bylaws, which are both different types of physical and data security, the ICANN org felt that the scope to be too big and the breadth too diverse to manage these distinctly different functions under one reporting structure. As the organization matured over the years, it became clear that these security related functions would be best managed in a distributed manner with specific and narrow responsibilities to be managed by the executive of the functional team best suited for the specified role. This decision was not made lightly and the org continues to evaluate and refine where these responsibilities lie. ICANN org made the decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN org is responsible. In addition, the org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. This body is therefore a mechanism that provides org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost.

Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject

Recommendation 2.3	
Recommendation text:	ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management (2.1 - 2.4) This recommendation can be considered implemented when ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations. This recommendation can be considered effective when ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	
Lead:	OCTO / E&IT
Summary of Public Comment:	Elements of support:

	• By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. • BC and IPC make specific statements of support for this grouping of recommendations, pointing to the SSR2 Review Team's assessment of SSR1 implementation as indicative as a reason the new position is warranted. • GAC believes "such a centralized role may have various benefits", however GAC notes it "would not wish to presume expertise in ICANN's internal administration of executive functions". • RySG notes support for this grouping of recommendations "insofar as they represent strategic requirements for ICANN Org risk management", however, RySG does not support the creation of a new position. Afnic offers its full support to the RySG's comment Elements of concern: • RySG, i2Coalition, Namecheap, and RrSG do not support creation of the new position called for in this grouping of recommendations. These commenters believe that the work specified in the role description is already being carried out by members of ICANN org, and it is not clear as to why the new position is needed in light of the existing work.
Dependencies:	Dependent on implementation of SSR2 recommendation 2.1.
Considerations:	Recommendations 2.1 - 2.4 should be treated as a group: It is not clear how this recommendation would improve current processes that are in place. ICANN has a centralized risk management function that manages a centralized risk assessment and mitigation process. This function is managed by a C-suite position (CFO). In their respective public comments on the draft report, ICANN org and Board encouraged the SSR2 RT to provide specific details as to what issues or risks the SSR2 RT identified with the current operations, how the recommendation would address these, and what metrics could be applied to assess implementation. As noted in ICANN org's public comment on the SSR2 draft report, because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages), ICANN org made the conscious decision to distribute the various security functions to the relevant functional areas within the organization. These functional teams work closely not only with one another but also with the Risk Committee of the Board, which provides oversight as to the risk based functions for which ICANN org is responsible.

	The ICANN org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. This body is therefore a mechanism that provides org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost. The Board has the oversight role not the authority to organize the structures of the ICANN org, which is a key aspect within the role of the ICANN CEO and part of his accountability. ICANN org is in a relatively unique state in regards to security management. There is the traditional role of data and systems security that most organizations have and protect against as well as the security and well-being of its staff. However, since ICANNthe org facilitates numerous meetings of scale with its communities and with its particular role in managing portions of the Internet's unique identifier systems as defined in its Bylaws, which are both different types of physical and data security, the ICANN org felt that the scope to be too big and the breadth too diverse to manage these distinctly different functions under one reporting structure. As the organization matured over the years, it became clear that these security related functions would be best managed in a distributed manner with specific and narrow responsibilities to be managed by the executive of the functional team best suited for the specified role. This decision was not made lightly and the org continues to evaluate and refine where these responsibilities lie. ICANN org made the decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN org is responsible. In addition, the org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. This body is therefore a mechanism that provides org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost.

Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject

Recommendation 2.4	
Recommendation text:	ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, supply chains for hardware and software, and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management (2.1 - 2.4) This recommendation can be considered implemented when ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations. This recommendation can be considered effective when ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	
Lead:	OCTO / E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● BC and IPC make specific statements of support for this grouping of recommendations, pointing to the SSR2 Review Team's assessment of SSR1 implementation as indicative as a reason the new position is warranted.

	• GAC believes "such a centralized role may have various benefits", however GAC notes it "would not wish to presume expertise in ICANN's internal administration of executive functions". • RySG notes support for this grouping of recommendations "insofar as they represent strategic requirements for ICANN Org risk management", however, RySG does not support the creation of a new position. Afnic offers its full support to the RySG's comment Elements of concern: • RySG, i2Coalition, Namecheap, and RrSG do not support creation of the new position called for in this grouping of recommendations. These commenters believe that the work specified in the role description is already being carried out by members of ICANN org, and it is not clear as to why the new position is needed in light of the existing work.
Dependencies:	Dependent on implementation of SSR2 recommendation 2.1.
Considerations:	Recommendations 2.1 - 2.4 should be treated as a group: It is not clear how this recommendation would improve current processes that are in place. In their respective public comments on the draft report, ICANN org and Board encouraged the SSR2 RT to provide specific details as to what issues or risks the SSR2 RT identified with the current operations, how the recommendation would address these, and what metrics could be applied to assess implementation. As noted in ICANN org's public comment on the SSR2 draft report, because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages), ICANN org made the conscious decision to distribute the various security functions to the relevant functional areas within the organization. These functional teams work closely not only with one another but also with the Risk Committee of the Board, which provides oversight as to the risk based functions for which ICANN org is responsible. The Board has the oversight role not the authority to organize the structures of the ICANN org, which is a key aspect within the role of the ICANN CEO and part of his accountability. ICANN org is in a relatively unique state in regards to security management. There is the traditional role of data and systems security that most organizations have and protect against as well as the security and well-being of its staff. However, since ICANNthe org facilitates numerous meetings of scale with its communities and with its particular role in managing portions of the Internet's unique identifier systems as defined in its Bylaws, which are both different types of physical and data security, the ICANN org felt that the scope to be too big and the breadth too diverse to manage these distinctly different functions under one reporting structure. As the organization matured over the years, it became clear

	that these security related functions would be best managed in a distributed manner with specific and narrow responsibilities to be managed by the executive of the functional team best suited for the specified role. This decision was not made lightly and the org continues to evaluate and refine where these responsibilities lie. ICANN org made the decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN org is responsible. In addition, the org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. This body is therefore a mechanism that provides org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject

SSR2 Recommendation 3: Improve SSR-Related Budget Transparency

Recommendation 3.1	
Recommendation text:	The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 3: Improve SSR-related Budget Transparency (3.1 - 3.3) This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	OCTO / E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. INTA further emphasizes that it "strongly supports" this grouping of recommendations and encourages the Board to consider them as high priority. ● GAC notes support for this grouping of recommendations. ● RySG "supports the recommended actions to improve SSR-related budget transparency", but does not support the creation of the new C-Suite position. Elements of concern: ● i2Coalition, Namecheap, and RrSG believe that ICANN is already dedicating resources to the efforts described in this grouping of recommendations. These commenters believe that the SSR2 Review Team does not adequately explain how the ongoing activities are insufficient. ● RySG does not support the creation of the new C-Suite position. ● Namecheap believes that this grouping of recommendations will "result in significant costs without contemplating the impact on the limited ICANN

	budget", and as such recommends that the ICANN Board reject this grouping of recommendations.
Dependencies:	Dependent on implementation of SSR2 recommendation 2.1.
Considerations:	The SSR2 Review Team defined successful implementation of this recommendation to be: This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget." Therefore - this implies that if the C-Suite position is not in place, the recommendation would not be considered implemented regardless of the activities that ICANN org is already undertaking as noted in the considerations." ICANN org is already undertaking work towards improving budget transparency. For example, ICANN org's Operating and Financial Plans for FY22-26 (Five-Year) and FY22 (One-Year), includes "Appendix C: ICANN Security, Stability, and Resiliency (SSR) of the Unique Internet Identifiers''. This appendix states: "ICANN's deep commitment to SSR underscores an approach to the concept that is holistic and interwoven into daily operations. In other words, every function of ICANN org contributes to the overall SSR through its support of org's work to advance ICANN's Mission. However, this Appendix aims to articulate some of the specific areas that particularly focus on supporting the SSR of these unique Internet identifiers." There may be benefits to periodic communication on SSR activities and note this is already partially performed as part of the current annual planning process but could be enhanced consistently with the presumed intent of the recommendation 3.1. It appears that the successful implementation of Recommendation 3.1 depends on implementation of Recommendation 2. In light of this dependency, clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective in the event that the Board rejects Recommendation 2 regarding the Executive C-Suite Security Officer, and that portion of the recommendation cannot be achieved. Clarification from the SSR2 Implementation Shepherds as to if successful implementation of Recommendations 3.2 and 3.2 may be decoupled from the implementation Recommendation 2. The outcome of the engagement with the SSR2 Implementation Shepherds could inform the Board's decision on next steps and whether Recommendations 3.2 and 3.3 can be approved.
Possible clarifying questions:	• Please clarify what the granularity of those reports should be? • What SSR benefit does the SSR2 RT observe will result from this reporting frequency?

Proposed recommended Board action:	Pending, hold to seek clarity or further information

Recommendation 3.2	
Recommendation text:	The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN strategic plan goals and objectives. ICANN org should implement those mechanisms.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 3: Improve SSR-related Budget Transparency (3.1 - 3.3) This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Finance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. INTA further emphasizes that it "strongly supports" this grouping of recommendations and encourages the Board to consider them as high priority. ● GAC notes support for this grouping of recommendations. ● RySG "supports the recommended actions to improve SSR-related budget transparency", but does not support the creation of the new C-Suite position. Elements of concern: ● i2Coalition, Namecheap, and RrSG believe that ICANN is already dedicating resources to the efforts described in this grouping of recommendations. These commenters believe that the SSR2 Review Team does not adequately explain how the ongoing activities are insufficient.

	• RySG does not support the creation of the new C-Suite position. • Namecheap believes that this grouping of recommendations will "result in significant costs without contemplating the impact on the limited ICANN budget", and as such recommends that the ICANN Board reject this grouping of recommendations.
Dependencies:	Dependent on implementation of SSR2 recommendation 2.1.
Considerations:	The SSR2 Review Team defined successful implementation of this recommendation to be: This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget." Therefore - this implies that if the C-Suite position is not in place, the recommendation would not be considered implemented regardless of the activities that ICANN org is already undertaking as noted in the considerations." ICANN org is already undertaking work towards improving budget transparency. For example, ICANN org's Operating and Financial Plans for FY22-26 (Five-Year) and FY22 (One-Year), includes "Appendix C: ICANN Security, Stability, and Resiliency (SSR) of the Unique Internet Identifiers". This appendix states: "ICANN's deep commitment to SSR underscores an approach to the concept that is holistic and interwoven into daily operations. In other words, every function of ICANN org contributes to the overall SSR through its support of org's work to advance ICANN's Mission. However, this Appendix aims to articulate some of the specific areas that particularly focus on supporting the SSR of these unique Internet identifiers." Clarification from the SSR2 Implementation Shepherds as to if successful implementation of Recommendations 3.2 and 3.2 may be decoupled from the implementation Recommendation 2. The outcome of the engagement with the SSR2 Implementation Shepherds could inform the Board's decision on next steps and whether Recommendations 3.2 and 3.3 can be approved.
Possible clarifying questions:	• Seek clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective in the event that the Board rejects Recommendation 2 and that portion of the recommendation cannot be achieved.
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 3.3	
Recommendation text:	The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 3: Improve SSR-related Budget Transparency (3.1 - 3.3) This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget.
Owner (SSR2 assigned):	ICANN Board and ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Finance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. INTA further emphasizes that it "strongly supports" this grouping of recommendations and encourages the Board to consider them as high priority. ● GAC notes support for this grouping of recommendations. ● RySG "supports the recommended actions to improve SSR-related budget transparency", but does not support the creation of the new C-Suite position. Elements of concern: ● i2Coalition, Namecheap, and RrSG believe that ICANN is already dedicating resources to the efforts described in this grouping of recommendations. These commenters believe that the SSR2 Review Team does not adequately explain how the ongoing activities are insufficient. ● RySG does not support the creation of the new C-Suite position. ● Namecheap believes that this grouping of recommendations will "result in significant costs without contemplating the impact on the limited ICANN budget", and as such recommends that the ICANN Board reject this grouping of recommendations.
Dependencies:	Dependent on implementation of SSR2 recommendation 2.1, and dependent on the structure and linkage as defined in recommendation 3.2

Considerations:	Much of requested content exists and can be adjusted to accommodate desired reporting parameters with further clarification in the implementation phase. SSR-related elements are included in ICANN's Five Year Operating & Financial Plan and Annual Operating Plan and Budget, and the Five Year Strategic Plan. Extensive public consultation activities are in place with regard to these documents. See, for example, information about ICANN's strategic planning process and the most recent Public Comment proceeding on the draft Five-Year Operating & Financial Plan and draft Operating Plan & Budget. In order to take dispositive action on this recommendation, ICANN org recommends that the Board seek clarification from the implementation shepherds as to whether this recommendation can be decoupled from the SSR2 Review Team's measure of success which references the C-Suite position from SSR2 recommendation 2.1-2.4. Note that recommendation 2.1-2.4 is proposed for Reject.
Possible clarifying questions:	• SSR-related elements are included in ICANN's Five Year Operating & Financial Plan and Annual Operating Plan and Budget, and the Five Year Strategic Plan. Extensive public consultation activities are in place with regard to these documents. See, for example, information about ICANN's strategic planning process and the most recent Public Comment proceeding on the draft Five-Year Operating & Financial Plan and draft Operating Plan & Budget. Can the implementation shepherds clarify what additional work beyond what is already in place should be done to meet the requirements of the recommendation?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

SSR2 Recommendation 4: Improve Risk Management Processes and Procedures

Recommendation 4.1	
Recommendation text:	ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3) This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Risk mgmt.
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC considers this grouping of recommendations to be top priority. ● In addition to its overarching support for all recommendations in the SSR2 Final Report, IPC specifies that it "concurs with the goal[s] of the recommendation[s] to prevent and address internal risks, and to adopt common industry standards". ● GAC notes support for this grouping of recommendations. ● In addition to its overarching support for all recommendations in the SSR2 Final Report, ALAC "strongly supports" the recommendation believes that "creating a centralized risk management function and adopting a recognized risk management standard (ISO 31000) would bring ICANN into alignment with best practices, both in technology-centric organizations and beyond. However, ICANN needs to recognize the unique risks and risk management challenges that ICANN faces due to its unique mandate and structure, in particular its policy development processes. ICANN's risk management

	structure must ensure that all risks are considered, including community participation that is balanced in order to avoid risks of capture, disproportionate influence by parties with less at stake and/or the ability to stagnate processes". ● RrSG supports Recommendation 4.2 "with the understanding that it will be narrowly tailored, specifically focused, and necessary to achieve the goals of the recommendation". Elements of concern: ● RySG, i2Coalition, Namecheap, and RrSG cite concerns about the elements of this grouping of recommendations that ask for a new role to be created that already exists in ICANN org, without providing explanation as to how the current activities are insufficient. For example, RySG believes that risk management at ICANN can be achieved "within the current staff structures without the addition of a C-Suite level position". ● RrSG does not support recommendation 4.1 as "the goal of this recommendation is not clear"
Dependencies:	n/a
Considerations:	● ICANN org believes the measures of success as outlined by the SSR2 are fully met by existing work. ● ICANN org already has a centralized risk management framework and function run by a dedicated person. The specific approach may not be exactly the same, but there is effectively nothing in these recommendations that is not already operational in the org. ● The Framework is clearly articulated and has been reconciled with the strategic plan for Fiscal Years 2021 - 2025. Those two items have been done subject to oversight of the Board Risk Committee and full Board. ● It is not clear if the SSR2 RT considered the briefings, background material, or responses to information requests about work underway when finalizing its recommendations. Several briefings delivered to the SSR2 RT throughout the duration of the review and in the ICANN org comments on the draft report. ● Significant resources are already dedicated to the above efforts.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 4.2	
Recommendation text:	ICANN org should adopt and implement ISO 31000 “Risk Management” and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures).
SSR2-defined measures of success:	Applies to SSR2 Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3) This recommendation can be considered implemented when ICANN org’s risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Risk mgmt.
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC considers this grouping of recommendations to be top priority. ● In addition to its overarching support for all recommendations in the SSR2 Final Report, IPC specifies that it “concurs with the goal[s] of the recommendation[s] to prevent and address internal risks, and to adopt common industry standards”. ● GAC notes support for this grouping of recommendations. ● In addition to its overarching support for all recommendations in the SSR2 Final Report, ALAC “strongly supports” the recommendation believes that “creating a centralized risk management function and adopting a recognized risk management standard (ISO 31000) would bring ICANN into alignment with best practices, both in technology-centric organizations and beyond. However, ICANN needs to recognize the unique risks and risk management challenges that ICANN faces due to its unique mandate and structure, in

	particular its policy development processes. ICANN's risk management structure must ensure that all risks are considered, including community participation that is balanced in order to avoid risks of capture, disproportionate influence by parties with less at stake and/or the ability to stagnate processes". ● RrSG supports Recommendation 4.2 "with the understanding that it will be narrowly tailored, specifically focused, and necessary to achieve the goals of the recommendation". Elements of concern: ● RySG, i2Coalition, Namecheap, and RrSG cite concerns about the elements of this grouping of recommendations that ask for a new role to be created that already exists in ICANN org, without providing explanation as to how the current activities are insufficient. For example, RySG believes that risk management at ICANN can be achieved "within the current staff structures without the addition of a C-Suite level position". ● RrSG does not support recommendation 4.1 as "the goal of this recommendation is not clear"
Dependencies:	n/a
Considerations:	ICANN org has a centralized risk management function and risk management framework in place that is based on the most commonly accepted best practices set by the COSO framework and aligns with the ICANN Strategic Plan for Fiscal Years 2021 - 2025 and includes defined measures of success. As ICANN org noted in its comment on the SSR2 Review Team draft report the main elements and outcomes of ISO 31000 are included in ICANN org's risk management framework. Under the framework, ICANN org uses its own in-house resources to achieve the same outcomes in a fit-for-purpose way. The Board Risk Committee (BRC) is responsible for oversight of ICANN implemented policies designed to manage ICANN's risk profile, including the establishment and implementation of standards, controls, limits and guidelines related to risk assessment and risk management. The BRC most recently reviewed the status of the risk management target model (Model) during its 13 April 2021 meeting. The Model was developed in 2014-2015 by ICANN org, the BRC, and external consultants, and agreed by the Board. ICANN org's then Risk Management program was benchmarked to the Model and the gaps identified. Over the past few years, ICANN org has worked to close those gaps. ICANN org has a strong, clearly documented risk management program, but not as envisioned by SSR2, as written. Thus, ICANN org agrees with the recommendation in principle, and considers the intent of the recommendation achieved through ICANN org current operations. However, the the portion of the recommendation that specifies that ICANN org "adopt and implement ISO 31000 'Risk Management' and validate its implementation with appropriate independent audits…" is not feasible because it is not clear what risks would be mitigated , nor what benefit would be

	derived in expanding significant resources to switch from the current risk-management process. The Board could not support for ICANN org's risk management operations already in place and encourage ICANN org to continue following industry best practices and look for ways to strengthen its risk management practices as it evolves its operations as part of its continuous improvement.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject because the recommendation cannot be approved in full.

Recommendation 4.3	
Recommendation text:	ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications).
SSR2-defined measures of success:	Applies to SSR2 Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3) This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.
Owner (SSR2 assigned):	ICANN org

Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Risk mgmt.
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC considers this grouping of recommendations to be top priority. ● In addition to its overarching support for all recommendations in the SSR2 Final Report, IPC specifies that it "concurs with the goal[s] of the recommendation[s] to prevent and address internal risks, and to adopt common industry standards". ● GAC notes support for this grouping of recommendations. ● In addition to its overarching support for all recommendations in the SSR2 Final Report, ALAC "strongly supports" the recommendation believes that "creating a centralized risk management function and adopting a recognized risk management standard (ISO 31000) would bring ICANN into alignment with best practices, both in technology-centric organizations and beyond. However, ICANN needs to recognize the unique risks and risk management challenges that ICANN faces due to its unique mandate and structure, in particular its policy development processes. ICANN's risk management structure must ensure that all risks are considered, including community participation that is balanced in order to avoid risks of capture, disproportionate influence by parties with less at stake and/or the ability to stagnate processes". ● RrSG supports Recommendation 4.2 "with the understanding that it will be narrowly tailored, specifically focused, and necessary to achieve the goals of the recommendation". Elements of concern: ● RySG, i2Coalition, Namecheap, and RrSG cite concerns about the elements of this grouping of recommendations that ask for a new role to be created that already exists in ICANN org, without providing explanation as to how the current activities are insufficient. For example, RySG believes that risk management at ICANN can be achieved "within the current staff structures without the addition of a C-Suite level position". ● RrSG does not support recommendation 4.1 as "the goal of this recommendation is not clear"
Dependencies:	SSR2 recommendation 2.
Considerations:	The term "security risk management" is not a standard risk management term. Based on this and some of the other recommendations, it appears that the SSR2

	team is conflating Risk Management and Information Security. ICANN has a responsible person in charge of risk management and a responsible person in charge of information security. Both of these people already report to C-level executives responsible for risk management and information security, the CFO and CIO, respectively. The recommendation to create a C-Suite position does not seem to take into account that there are already responsible C-level executives. The Risk Management function already "regularly update, and report on, a register of security risks and guide ICANN org's activities." The org has Cyber Security Frameworks in place which have been regularly reviewed by outside firms. It is not clear how this does not satisfy the recommendation. Clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective in the event that the Board rejects Recommendation 2 regarding the Executive C-Suite Security Officer, and that portion of the recommendation cannot be achieved. It is not clear as to what would be mitigated, nor what cost/benefit would be derived because the SSR2 Review Team has not articulated the current problem or a gap, nor how the desired outcome is envisioned. ICANN org made the decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN org is responsible. In addition, the org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. This body is therefore a mechanism that provides org with the overarching perspective and ability to centrally act on all security matters.
Possible clarifying questions:	• Seek clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective in the event that the Board rejects Recommendation 2 and that portion of the recommendation cannot be achieved.
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications

Recommendation 5.1	
Recommendation text:	ICANN org should implement an ISMS and be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4) This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC and ALAC specifically call out this grouping of recommendations as “top priority”, and “strong[ly] support”, respectively. ● GAC notes support for this grouping of recommendations. ● RrSG notes that it “generally supports certification, auditing, and reporting of ICANN.” Elements of concern: n/a
Dependencies:	n/a

Considerations:	ICANN org is currently following industry-specific security standards and best practices and is in the process of migrating to the NIST Cybersecurity Framework with oversight from the Risk Committee of the Board. ICANN org is transitioning to NIST CSF. Once this transition is complete, org believes the measures of success as outlined by the SSR2 will be met.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 5.2	
Recommendation text:	Based on the ISMS, ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4) This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	

Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC and ALAC specifically call out this grouping of recommendations as “top priority”, and “strong[ly] support”, respectively. ● GAC notes support for this grouping of recommendations. ● RrSG notes that it “generally supports certification, auditing, and reporting of ICANN.” Elements of concern: n/a"
Dependencies:	Dependent on implementation of SSR2 recommendation 5.1.
Considerations:	ICANN org is currently following industry-specific security standards and best practices and is in the process of migrating to the NIST Cybersecurity Framework with oversight from the Risk Committee of the Board. Work is already underway towards full implementation of this recommendation.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 5.3	
Recommendation text:	ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4) This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and

	adequately addresses current security threats and offers plans to address potential future security threats.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	E&IT, Procurement
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC and ALAC specifically call out this grouping of recommendations as "top priority", and "strong[ly] support", respectively. ● GAC notes support for this grouping of recommendations. ● RrSG notes that it "generally supports certification, auditing, and reporting of ICANN." Elements of concern: n/a
Dependencies:	n/a
Considerations:	ICANN org's Engineering & Information Technology (E&IT) function already requires all vendors and service providers to have a risk assessment performed and documented which meet industry-standard requirements. Clarification from the SSR2 Implementation Shepherds should be sought as to if the SSR2 Review Team's intent was to expand this risk assessment to all ICANN org vendors and service providers in order to accurately assess resource requirements and feasibility. ICANN org recommends further engagement with the SSR2 Implementation Shepherds for clarification on the intended scope of the recommendation.
Possible clarifying questions:	● All services onboarded through the Engineering and Information Technology function at ICANN org are required to have a Risk Assessment performed and documented. This risk assessment is used for the business to assess the risks of using those external services. Is the intention of the recommendation to expand risk assessment resources to all ICANN org services?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 5.4	
Recommendation text:	ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes to manage risk, security, and vulnerabilities.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4) This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC and ALAC specifically call out this grouping of recommendations as “top priority”, and “strong[ly] support”, respectively. ● GAC notes support for this grouping of recommendations. ● RrSG notes that it “generally supports certification, auditing, and reporting of ICANN.” ● RySG in reference to recommendation 5.4 suggests “that the Board seek additional clarity from the SSR2 RT regarding what entities beyond the ICANN community ICANN Org should report out regarding its security activities” Elements of concern: n/a

Dependencies:	n/a
Considerations:	ICANN org recommends further engagement with the SSR2 Implementation Shepherds for clarification on detailed elements of the reports and what is envisioned to report out “beyond” the ICANN community for this recommendation. Clarification needs to be sought on several elements of this recommendation in order to accurately assess resource requirements and enable approval. For example granularity of the reports expected by the SSR2 Review Team’s expected, and what entities the SSR2 Review Team envisioned ICANN org report out to “beyond” the ICANN community are not clear.
Possible clarifying questions:	a. Please clarify the SSR2 RT’s expectations of granularity of the reports? b. What additional steps, beyond publishing the reports to ICANN org, does the SSR2 recommendation intend ICANN org to take?
Proposed recommended Board action:	Pending, likely to be approved once further information is gathered to enable approval.

SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency

Recommendation 6.1	
Recommendation text:	ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency (6.1 - 6.2) This recommendation can be considered implemented when ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting. These recommendations can be considered effective when ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC specifically notes its “strong support” for this grouping of recommendations. ● GAC notes support for this grouping of recommendations. ● While RySG “supports its members adopting vulnerability disclosure policies as good business practice, it does not support ICANN acting as a clearinghouse, gatekeeper, or regulator of vulnerability disclosure policies”. Elements of concern: ● RySG, Namecheap, and RrSG explicitly note that they do not support this grouping of recommendations. These commenters believe elements of the recommendations contemplate that ICANN org should unilaterally make modifications to the Registrar Accreditation Agreement (RAA). For example, Namecheap notes: “According to the RAA (which is binding on ICANN and each accredited registrar), the sole process to negotiate and modify the RAA is

	detailed in Section 7.4 of the RAA. It is a process between ICANN Org and the Registrar Stakeholder Group (RrSG), and can only be initiated by those parties. Those are the only parties that participate in the negotiations. Although any draft revisions are subject to public comment, the RrSG is under no obligation to accept any public comment". ● While IPC is supportive of this grouping of recommendations, IPC believes that requir[ing] dotBrands to disclose all vulnerabilities in their business to ICANN...goes beyond ICANN's remit. At a minimum, any vulnerabilities should be limited only to those systems directly related to the operation of the TLD." ● While they do not specifically reference this grouping of recommendations, Tucows and PIR note concern in their overarching comments to the SSR2 Final Report that some recommendations ask ICANN org to make unilateral changes to the Registry Agreement and Registrar Accreditation Agreement. PIR expresses that "changes to Registry Agreements of this sort should only be made via the GNSO Policy Development Process resulting in a Consensus Policy or via triggering a formal negotiation process under the terms of the Registry Agreement." ● Tucows "notes the long-term efforts that the Registrars and Registries have undertaken with ICANN Org in order to attempt to negotiate new contractual clauses that other ICANN Community-led efforts have recommended including", and believes that only ICANN org and the Contracted Party House should be involved in the contract negotiation process.
Dependencies:	n/a
Considerations:	The 2nd half of this rec is difficult. Not clear what "prove insufficient" would mean in a measurable sense and moving this into contracts will require the contracted parties to agree. It is not clear if elements of this recommendation are seeking potential contract modifications. Contract changes would require either policy work to be initiated by the GNSO or contractually mandated contract negotiations. In order for the Board to take dispositive action on this recommendation, clarification is required from the implementation shepherds. Elements of this recommendation that require further clarification include how SSR best practices/objectives should be identified? How ICANN should measure adoption? How ICANN can unilaterally impose a requirement to adopt best practices/objectives in contracts, agreements, and MOUs? What it means for org's promotion efforts to be considered insufficient and what happens if the contracted parties oppose new language in their contracts? As written, what ICANN org should do in the event there is not voluntary adoption does not make sense. Possibly, the review team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and MOUs" - this should be clarified with the implementation shepherds. If this is the

	intent,this would likely be a policy matter and not something ICANN can unilaterally impose in “contracts, agreements, and MOUs.”
Possible clarifying questions:	● Is the intent of the SSR2 RT that ICANN org promotes voluntary adoption of two things ("SSR best practices” _AND_ “objectives for vulnerability disclosures”) or one thing (SSR vulnerability disclosure best practices and objectives)? ● In either case, is it the intent of SSR2 RT that ICANN org develop these resources for voluntary adoption or make use of already developed resources? If the latter, can the implementation shepherds provide references to those resources? ● How should adoption of the voluntary measures be measured? ● Who should determine whether the voluntary measures are sufficiently or insufficiently adopted? ● Assuming the statement "ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs” should be interpreted to read “ICANN Org should require contracted parties to implement the best practices and objectives via contracts, agreements, and MOUs”, is it the intent of the SSR2 RT for ICANN org to modify existing contracts, agreements, and MOUs to require this implementation or is the intent that future contracts, agreements, and MOUs include this requirement?
Proposed recommended Board action:	Pending, likely to be rejected unless additional information shows implementation is feasible.

Recommendation 6.2	
Recommendation text:	ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency (6.1 - 6.2) This recommendation can be considered implemented when ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting.

	These recommendations can be considered effective when ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	GDS
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC specifically notes its "strong support" for this grouping of recommendations. ● GAC notes support for this grouping of recommendations. ● While RySG "supports its members adopting vulnerability disclosure policies as good business practice, it does not support ICANN acting as a clearinghouse, gatekeeper, or regulator of vulnerability disclosure policies". Elements of concern: ● RySG, Namecheap, and RrSG explicitly note that they do not support this grouping of recommendations. These commenters believe elements of the recommendations contemplate that ICANN org should unilaterally make modifications to the Registrar Accreditation Agreement (RAA). For example, Namecheap notes: "According to the RAA (which is binding on ICANN and each accredited registrar), the sole process to negotiate and modify the RAA is detailed in Section 7.4 of the RAA. It is a process between ICANN Org and the Registrar Stakeholder Group (RrSG), and can only be initiated by those parties. Those are the only parties that participate in the negotiations. Although any draft revisions are subject to public comment, the RrSG is under no obligation to accept any public comment". ● While IPC is supportive of this grouping of recommendations, IPC believes that requir[ing] dotBrands to disclose all vulnerabilities in their business to ICANN...goes beyond ICANN's remit. At a minimum, any vulnerabilities should be limited only to those systems directly related to the operation of the TLD." ● While they do not specifically reference this grouping of recommendations, Tucows and PIR note concern in their overarching comments to the SSR2 Final Report that some recommendations ask ICANN org to make unilateral changes to the Registry Agreement and Registrar Accreditation Agreement. PIR expresses that "changes to Registry Agreements of this sort should only be made via the GNSO Policy Development Process resulting in a Consensus

	Policy or via triggering a formal negotiation process under the terms of the Registry Agreement." ● Tucows "notes the long-term efforts that the Registrars and Registries have undertaken with ICANN Org in order to attempt to negotiate new contractual clauses that other ICANN Community-led efforts have recommended including", and believes that only ICANN org and the Contracted Party House should be involved in the contract negotiation process.
Dependencies:	n/a
Considerations:	● Implementing a new coordinated vulnerability disclosure reporting framework may require considerable time and resources (community involvement?). Additionally, if contract changes are required, this requires either policy work or contract negotiations. ● It is not clear how the existing Coordinated Vulnerability Disclosure Reporting framework does not meet this recommendation (https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf; see also: https://www.icann.org/en/blogs/details/icann-coordinated-disclosure-guidelines-11-3-2013-en ● Additionally, as noted by the RySG, if the SSR2 RT is recommending global contractual changes, this can only come about via Consensus Policy or Contract Negotiations. ● "Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue)." It is not clear how the reporting of breaches or other "SSR-related issues" to ICANN org would occur, through what process, in compliance with national laws, or how implementation would help or mitigate issues for those affected or required to fix the given issue? ● "ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure." - this component of the recommendation is met by existing work. There are three components of this recommendation, which have different considerations. There is a risk in splitting components of a recommendation in that the Bylaws do not provide the option of modifying recommendations.: ● "ICANN org should implement coordinated vulnerability disclosure reporting." - this component of the recommendation is met by existing work. ● "Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue)." It is not clear how the reporting of breaches or other "SSR-related issues" to ICANN org would occur, through what process, in compliance with national

	laws, or how implementation would help or mitigate issues for those affected or required to fix the given issue? ● "ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure." - this component of the recommendation is met by existing work. ICANN org has a Coordinated Vulnerability Disclosure Reporting framework in place: (https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf; ● See also: https://www.icann.org/en/blogs/details/icann-coordinated-disclosure-guidelines-11-3-2013-en In order for the Board to take dispositive action, ICANN org recommends further consultation with the SSR2 Implementation Shepherds on this recommendation to better understand the intent of the recommendation.
Possible clarifying questions:	● Can the SSR2 implementation shepherds provide further details as to how the existing Coordinated Vulnerability Disclosure framework is insufficient? That is, what issue(s) regarding the existing framework were discussed over the course of the SSR2's deliberations? ● Can the SSR2 implementation shepherds provide further details regarding the SSR2's understanding of how the reporting of breaches or other "SSR-related issues" to ICANN org would be helping those affected or required to fix the given issue? ● Can the SSR2 implementation shepherds provide any more guidance on what the SSR2 sees as constituting an "SSR-related issue" that should be included in required disclosure from a contracted party to ICANN, other than breach?
Proposed recommended Board action:	Pending, likely to be rejected unless additional information shows implementation is feasible.

SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures

Recommendation 7.1	
Recommendation text:	ICANN org should establish a Business Continuity Plan for all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5) This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	
Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC and BC make additional comments as noted below. ● BC and M3AAWG understand that ICANN org lacks a Business Continuity and Disaster Recovery Plan, and as such believe implementation of this grouping of recommendations should be a priority. ● ALAC "strongly supports" this grouping of recommendations and believes it "support[s] the overarching theme of bringing ICANN into alignment with InfoSec and operational security standards prevalent in technology-centric organizations worldwide". ● GAC notes support for this grouping of recommendations. ● RySG notes that while it "supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan", however RySG has concerns about the scope of the recommendation. Elements of concern:

	● RySG believes the "scope of 'all the systems owned by or under the ICANN org purview' is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes". ● RySG recommends "that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators".
Dependencies:	n/a
Considerations:	Recommendations 7.1, 7.2, 7.3, 7.5 pertain to Business Continuity and Disaster Recovery and should be treated as a grouping. Additional clarification will be necessary to determine the scope of ISO 22301 in comparison to operational plans for systems disaster recovery to support operational business continuity. Community comments from RySG highlight scope concerns - some further engagement with the community, or clarifications could be sought. ICANN org recommends further clarification from the SSR2 implementation shepherds as to whether this recommendation can be decoupled from the SSR2 Review Team's measure of success for recommendation 7.4 requirement that "a non-U.S., non-North American site is operational." (see SSR2 rec 7.4)
Possible clarifying questions:	ICANN org reading of this recommendation is that the SSR2 RT has conflated the goal of Business Continuity Management for the whole of ICANN org, such as what ISO 22301 calls for, with the goals of operational plans for systems disaster recovery to support operational business continuity. In light of ICANN org's interpretation, can the implementation shepherds please clarify the intent of this recommendation?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 7.2	
Recommendation text:	ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO).

SSR2-defined measures of success:	Applies to SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5) This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America. ICANN org recommends further clarification from the SSR2 implementation shepherds as to whether this recommendation can be decoupled from the SSR2 Review Team's measure of success for recommendation 7.4 requirement that "a non-U.S., non-North American site is operational." (see SSR2 rec 7.4)
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	
Lead:	IANA
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC and BC make additional comments as noted below. ● BC and M3AAWG understand that ICANN org lacks a Business Continuity and Disaster Recovery Plan, and as such believe implementation of this grouping of recommendations should be a priority. ● ALAC "strongly supports" this grouping of recommendations and believes it "support[s] the overarching theme of bringing ICANN into alignment with InfoSec and operational security standards prevalent in technology-centric organizations worldwide". ● GAC notes support for this grouping of recommendations. ● RySG notes that while it "supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan", however RySG has concerns about the scope of the recommendation. Elements of concern: ● RySG believes the "scope of 'all the systems owned by or under the ICANN org purview' is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an

	overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes". ● RySG recommends "that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators".
Dependencies:	n/a
Considerations:	Recommendations 7.1, 7.2, 7.3, 7.5 pertain to Business Continuity and Disaster Recovery and should be treated as a grouping. Scope requires clarification from the implementation shepherds. A DR already exists, it's owned by E&IT. We in IANA are unsure of ISO27031 and therefore cannot comment if the current DR is in line with this standard. The recommendation could be interpreted to be wide or narrow (like, does it include the root server operators, verisign, etc?) and ICANN org has to come to alignment on what exactly is in scope here. See: https://wecann.icann.org/docs/DOC-9184 for current DR plan which clearly shows it includes IANA. Unsure as to why the response from the RT still says they haven't received any plans since 2017? Perhaps this is why the recc is still here?
Possible clarifying questions:	The recommendation states "... includes all relevant systems that contribute to the security and stability of the DNS". Does the SSR2 RT mean systems owned by ICANN org? Or does this recommendation envisage ICANN being responsible for developing plans for systems it does not operate?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 7.3	
Recommendation text:	ICANN org should also establish a DR plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5) This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational.

	This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	
Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC and BC make additional comments as noted below. ● BC and M3AAWG understand that ICANN org lacks a Business Continuity and Disaster Recovery Plan, and as such believe implementation of this grouping of recommendations should be a priority. ● ALAC "strongly supports" this grouping of recommendations and believes it "support[s] the overarching theme of bringing ICANN into alignment with InfoSec and operational security standards prevalent in technology-centric organizations worldwide". ● GAC notes support for this grouping of recommendations. ● RySG notes that while it "supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan", however RySG has concerns about the scope of the recommendation. Elements of concern: ● RySG believes the "scope of 'all the systems owned by or under the ICANN org purview' is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes". ● RySG recommends "that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators".
Dependencies:	n/a
Considerations:	Recommendations 7.1, 7.2, 7.3, 7.5 pertain to Business Continuity and Disaster Recovery and should be treated as a grouping. SSR2 specifies ISO 27031 in this recommendation. ICANN Org has already commenced adoption of NIST standards.

	Community comments from RySG highlight scope concerns - some further engagement with the community, or clarifications could be sought ICANN org recommends further clarification from the SSR2 implementation shepherds as to whether this recommendation can be decoupled from the SSR2 Review Team's measure of success for recommendation 7.4 requirement that "a non-U.S., non-North American site is operational." (see SSR2 rec 7.4)
Possible clarifying questions:	The recommendation specifies ISO 27031. ICANN org has already commenced adoption of NIST standards. Did the SSR2 RT consider if other standards such as NIST SP 800-34 Rev 1 would meet the requirements of the recommendation?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 7.4	
Recommendation text:	ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5) This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	

Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC and BC make additional comments as noted below. ● BC and M3AAWG understand that ICANN org lacks a Business Continuity and Disaster Recovery Plan, and as such believe implementation of this grouping of recommendations should be a priority. ● ALAC "strongly supports" this grouping of recommendations and believes it "support[s] the overarching theme of bringing ICANN into alignment with InfoSec and operational security standards prevalent in technology-centric organizations worldwide". ● GAC notes support for this grouping of recommendations. ● RySG notes that while it "supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan", however RySG has concerns about the scope of the recommendation. Elements of concern: ● RySG believes the "scope of 'all the systems owned by or under the ICANN org purview' is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes". ● RySG recommends "that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators".
Dependencies:	n/a
Considerations:	Clarification is needed on what the Review Team is trying to specifically achieve by this would be helpful, and are they focused on the KSK (hence they mention culpepper) or on ICANN corporate systems? The Cost benefit of the new site is not clear from the SSR2 report. Implementation of this recommendation as written is not currently feasible for some portions of the IANA functions. Specifically, Section 4.2 of the IANA Naming Function Contract that prohibits IANA operations outside of the United States, These restrictions could be removed through contract amendments if there were a desire to do so from the ICANN community, which would require community consultation and discussion.
Possible clarifying questions:	● What did the SSR2 RT consider would be the likelihood of an incident that impacts the whole of the United States or North America? ● The recommendation mentions Culpeper. Culpeper is only used as a KSK facility. ICANN has 2 KSK facilities; Culpeper and El Segundo. ICANN has corporate data center locations elsewhere in DC and LA separate from KSK

	facilities. Does this recommendation mean the locations where the corporate infrastructure is located? Or the separate locations that house the KSK/IANA infrastructure? ● The majority of ICANN org corporate services (payroll, finance, DMS, CMS, email, meeting services, etc.) are provided by third parties. Given that the majority of these outsourced services make up the backbone of business operations for ICANN org, can the implementation shepherds please clarify why having an additional DR site outside of U.S. territory provide enough of an added benefit to justify the additional cost?
Proposed recommended Board action:	Pending, likely to be rejected unless additional information shows implementation is feasible.

Recommendation 7.5	
Recommendation text:	ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5) This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium-high
ICANN org assessment:	
Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC and BC make additional comments as noted below.

	● BC and M3AAWG understand that ICANN org lacks a Business Continuity and Disaster Recovery Plan, and as such believe implementation of this grouping of recommendations should be a priority. ● ALAC "strongly supports" this grouping of recommendations and believes it "support[s] the overarching theme of bringing ICANN into alignment with InfoSec and operational security standards prevalent in technology-centric organizations worldwide". ● GAC notes support for this grouping of recommendations. ● RySG notes that while it "supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan", however RySG has concerns about the scope of the recommendation. Elements of concern: ● RySG believes the "scope of 'all the systems owned by or under the ICANN org purview' is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes".
Dependencies:	Dependent on 7.4
Considerations:	Recommendations 7.1, 7.2, 7.3, 7.5 pertain to Business Continuity and Disaster Recovery and should be treated as a grouping. ICANN org recommends further clarification from the SSR2 implementation shepherds as to whether this recommendation can be decoupled from the SSR2 Review Team's measure of success for recommendation 7.4 requirement that "a non-U.S., non-North American site is operational." (see SSR2 rec 7.4)
Possible clarifying questions:	● Consult with the Implementation Shepherds to better understand elements of this recommendation that are not feasible as written, or are not clear, including if the SSR2 Review Team considered the benefit versus cost considerations
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties

Recommendation 8.1	
Recommendation text:	ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the DNS for end-users, businesses, and governments.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties (8.1) This recommendation can be considered implemented when ICANN org has included abuse and security specialists in these negotiations and the management of the domain name system aligns with public safety and consumer interests, and not just those of the domain name industry. This recommendation can be considered effective when a broader and more balanced set of stakeholders are able to have direct input into the contracts negotiated with contracted parties.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	GDS
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this recommendation. BC believes the recommendation should be top priority and ALAC emphasizes “strong support” for the recommendation. ● In addition to its support for all SSR2 recommendations, INTA specifically notes support for this recommendation, stating that “INTA has seen time and time again that the specific and explicit language of the contracts is paramount - ICANN refuses to enforce obligations unless they have an express basis to do so under the terms of the contracts, even if certain contracted party activity clearly violates the spirit of the provision and the intent of the community policy that was the basis for the contractual provisions. Therefore, it is equally paramount that ICANN include independent third-party negotiators that are free from conflicts of interest and represent the

	non-contracted participants of the ICANN community in contractual negotiations to ensure final contract provisions faithfully implement community policies and properly facilitate enforcement of these policies". ● M3AAWG supports the recommendation and its "objective of improving the SSR of the DNS for end-users, businesses, and governments." ● GAC agrees with the spirit of the recommendation, but recognises that "contract negotiations between ICANN and the Contracted Parties do not currently include third parties and therefore would encourage ICANN to consult with independent security experts (i.e. non-contracted entities) for the purposes of developing and agreeing upon security-related provisions that can be incorporated into the contracts". ● Article 19 asks that the recommendation be revised "to ensure that the process of selecting the negotiating team should be a multi-stakeholder process, and that the composition of the negotiating team must comprise various stakeholders from the Empowered Community." Elements of concern: ● RySG, PIR, Tucows, Namecheap, and RrSG believe that the recommendation is not consistent with the terms of the Registry Agreement and the Registrar Accreditation Agreement, and as such, believe the recommendation should be rejected. For example, RySG notes: "Section 7.7 of the Registry Agreement is the section that allows for the bilateral negotiation of a contemplated change to the Registry Agreement between Registries and ICANN itself, not third parties that are not a party to the Agreement, with one exception: The Registry Agreement considers the possibility of a 'Working Group' that may participate in these negotiations, but it is explicitly the registries that makes such an appointment, not ICANN". ● Further, Namecheap notes, "[a]ccording to the RAA (which is binding on ICANN and each accredited registrar), the sole process to negotiate and modify the RAA is detailed in Section 7.4 of the RAA. It is a process between ICANN Org and the Registrar Stakeholder Group (RrSG), and can only be initiated by those parties. Those are the only parties that participate in the negotiations''.
Dependencies:	n/a
Considerations:	ICANN org notes that the parties that registered disagreement with this recommendation through their public comments are the parties that would be involved in the types of negotiations addressed by this recommendation. ICANN org notes that the aspect of the recommendation that calls for the introduction of a third party into the bilateral negotiation process is not proper or feasible. The Registry Agreement, and Registrar Accreditation Agreement do not allow for third-party beneficiaries. ICANN org notes that it negotiates in the broader interest of ICANN, including the public interest, and does not represent the interests of the domain industry.

	ICANN org further notes that Recommendation 8.1 is not allowed under the provisions in existing agreements for how contract negotiations should be initiated and carried out, e.g., Registry Agreement Section 7.7). While the agreements do provide for a "Working Group", these have contractually specific meanings that are not aligned with this recommendation. For example, in the case of the RA, a "Working Group" is defined as: "representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements (excluding bilateral amendments pursuant to Section 7.6(i))."[1] Neither the Board or ICANN org is involved in the appointment of these contractual "Working Groups". Further, as the Board and ICANN org noted in their respective comments on the SSR2 Review Team draft report, the Board and ICANN org cannot bring about contractual changes unilaterally. If changes in provisions of the contracts are desired in order to address perceived gaps related to security, stability, and resiliency of the DNS for end-users, businesses, and governments, as referred to in Recommendation 8.1, then the Policy Development Process allows for such "independent experts" as mentioned in the recommendation to participate as those policy recommendations are developed. The Board and ICANN org take in the inputs of the community and strive to carefully reflect those inputs in the decisions made with ICANN org and Board, as an essential part of serving the public interest. It is difficult to contemplate bringing in a third party to do that. The Board could encourage ICANN to continue bilateral discussions with the contracted parties in a way that enhances the security, stability, and resiliency of the DNS and to strive to have these bilateral discussions be transparent to the general public, in order to continue building trust.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject because the recommendation cannot be approved in full.

[1] Base Registry Agreement - Updated 31 July 2017. Section 7.6(j)(v): https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

SSR2 Recommendation 9: Monitor and Enforce Compliance

Recommendation 9.1	
Recommendation text:	The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse-related obligations in contracts, baseline agreements, temporary specifications, and community policies.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4) This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).
Owner (SSR2 assigned):	ICANN Board
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Compliance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations, although IPC specifically notes support for this grouping of recommendations. BC further believes this grouping of recommendations should be top priority and INTA and ALAC emphasize “strong support” for this grouping of recommendations. ● M3AAWG and GAC note support for this grouping of recommendations. GAC notes “it is particularly concerning that ICANN Contractual Compliance would assert to the SSR2 Review Team in April 2018 - that ‘current contracts with registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus ineffective in allowing them to pursue those engaged in systemic DNS Abuse.’ This gap in the current contracts, identified by both ICANN Contract Compliance and the

	ICANN Board demonstrates the need for improved and enforceable provisions to address DNS Abuse". ● While Article 19 agrees with the objective of this grouping of recommendations, it "strongly oppose[s]" the "proposition to develop and deploy monitoring systems without strong due process procedures in place, including the creation of a clear timeline to take action against the domain name after providing the registrant with opportunities to explain their action. We also oppose any attempts to include content takedowns without due process." Elements of concern: ● RySG believes Recommendation 9.1 specifically to be "extremely vague and we reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars. Such a recommendation exceeds the scope of this Review". ● RySG disagrees with the "implication" of this grouping of recommendations that "ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement", and notes that "Registry Operators' compliance with the abuse obligations were recently audited by ICANN Compliance". ● PIR makes an overarching comment to the SSR2 final report that some "recommendations imply that ICANN Compliance is not enforcing existing contractual obligations or encourage ICANN Compliance to undertake activities that are clearly outside of ICANN Compliance's scope and remit." ● RrSG notes elements of concern about several individual recommendations in this grouping, as noted below: ● 9.1: "ICANN Contractual Compliance already performs this function through complaint processing, reviews, and audits. It is not clear to the RrSG what problem this recommendation is intended to fix". ● 9.2: "ICANN Compliance already proactively monitors compliance through audits and review, and additionally in light of complaint processing, does this". ● 9.3: "Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing". ● 9.4: "As part of ongoing collaboration between the RrSG and ICANN Contractual Compliance, the RrSG has requested ICANN Contractual Compliance make its needs for additional tools known to the RrSG on several occasions. The RrSG is not aware of any specific recommendations from ICANN Contractual Compliance".
Dependencies:	n/a
Considerations:	It is not clear what the SSR2 RT is requesting that ICANN Compliance perform, that is not currently being done in terms of enforcing the contracts and consensus policies.

	• ICANN Contractual Compliance current operations ensure that registries and registrars fulfill the requirements in their agreements with ICANN org. • Reporting and performance measurement metrics are published to icann.org. • Details regarding Registrar and Registry related Abuse complaints can be found in the monthly metrics published by Compliance. This includes the number of Registrar Abuse Complaints related to Pharming/Phishing, Malware/botnets, Spam, Counterfeiting, Fraud, Pharmaceuticals and Trademark etc. as well as number of complaints related to GAC Category 1 Safeguards. Measures of success as outlined by the SSR2 appear to be fully met by the noted existing work.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 9.2	
Recommendation text:	ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4) This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).

Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Compliance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations, although IPC specifically notes support for this grouping of recommendations. BC further believes this grouping of recommendations should be top priority and INTA and ALAC emphasize "strong support" for this grouping of recommendations. ● M3AAWG and GAC note support for this grouping of recommendations. GAC notes "it is particularly concerning that ICANN Contractual Compliance would assert to the SSR2 Review Team in April 2018 - that 'current contracts with registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus ineffective in allowing them to pursue those engaged in systemic DNS Abuse.' This gap in the current contracts, identified by both ICANN Contract Compliance and the ICANN Board demonstrates the need for improved and enforceable provisions to address DNS Abuse". ● While Article 19 agrees with the objective of this grouping of recommendations, it "strongly oppose[s]" the "proposition to develop and deploy monitoring systems without strong due process procedures in place, including the creation of a clear timeline to take action against the domain name after providing the registrant with opportunities to explain their action. We also oppose any attempts to include content takedowns without due process." Elements of concern: ● RySG believes Recommendation 9.1 specifically to be "extremely vague and we reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars. Such a recommendation exceeds the scope of this Review". ● RySG disagrees with the "implication" of this grouping of recommendations that "ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement", and notes that "Registry Operators' compliance with the abuse obligations were recently audited by ICANN Compliance". ● PIR makes an overarching comment to the SSR2 final report that some "recommendations imply that ICANN Compliance is not enforcing existing

	contractual obligations or encourage ICANN Compliance to undertake activities that are clearly outside of ICANN Compliance's scope and remit." ● RrSG notes elements of concern about several individual recommendations in this grouping, as noted below: ● 9.1: "ICANN Contractual Compliance already performs this function through complaint processing, reviews, and audits. It is not clear to the RrSG what problem this recommendation is intended to fix". ● 9.2: "ICANN Compliance already proactively monitors compliance through audits and review, and additionally in light of complaint processing, does this". ● 9.3: "Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing". ● 9.4: "As part of ongoing collaboration between the RrSG and ICANN Contractual Compliance, the RrSG has requested ICANN Contractual Compliance make its needs for additional tools known to the RrSG on several occasions. The RrSG is not aware of any specific recommendations from ICANN Contractual Compliance".
Dependencies:	n/a
Considerations:	Elements of this recommendation require clarification regarding how the Review Team understands Compliance can perform the requested actions, including the authority it believes Compliance has to carry out the actions. Similar to CCT. Pending EPDP. "should include the validation of address fields and conducting periodic audits of the accuracy of registration data" seems to imply WHOIS ARS, which is currently on hold. For actions that are not included in the current RAA, it's not clear how the SSR2 believes Compliance can perform these actions including the authority it believes Compliance has to carry out these actions. ICANN org does not have authority to require validation beyond what is in the Registry Agreement and Registrar Accreditation Agreement. Elements of this recommendation require clarification regarding how the Review Team understands Compliance can perform the requested actions, including the authority it believes Compliance has to carry out the actions.
Possible clarifying questions:	● Compliance enforces RAA obligations related to accuracy of registration data (see [LINK] with whois inaccuracy metrics). Please clarify what this recommendation seeks from Compliance beyond what the function currently performs in this area? ● For actions that are not included in the current RAA, please explain how the SSR2 RT believes Compliance can perform these actions including the authority it believes Compliance has to carry out these actions.

Proposed recommended Board action:	Pending, likely to be rejected unless additional information shows implementation is feasible.

Recommendation 9.3	
Recommendation text:	ICANN org should have compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4) This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Compliance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations, although IPC specifically notes support for this grouping of recommendations. BC further believes this grouping of recommendations should be top priority and INTA and ALAC emphasize “strong support” for this grouping of recommendations. ● M3AAWG and GAC note support for this grouping of recommendations. GAC notes “it is particularly concerning that ICANN Contractual Compliance would assert to the SSR2 Review Team in April 2018 - that ‘current contracts with

	registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus ineffective in allowing them to pursue those engaged in systemic DNS Abuse.' This gap in the current contracts, identified by both ICANN Contract Compliance and the ICANN Board demonstrates the need for improved and enforceable provisions to address DNS Abuse". ● While Article 19 agrees with the objective of this grouping of recommendations, it "strongly oppose[s]" the "proposition to develop and deploy monitoring systems without strong due process procedures in place, including the creation of a clear timeline to take action against the domain name after providing the registrant with opportunities to explain their action. We also oppose any attempts to include content takedowns without due process." Elements of concern: ● RySG believes Recommendation 9.1 specifically to be "extremely vague and we reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars. Such a recommendation exceeds the scope of this Review". ● RySG disagrees with the "implication" of this grouping of recommendations that "ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement", and notes that "Registry Operators' compliance with the abuse obligations were recently audited by ICANN Compliance". ● PIR makes an overarching comment to the SSR2 final report that some "recommendations imply that ICANN Compliance is not enforcing existing contractual obligations or encourage ICANN Compliance to undertake activities that are clearly outside of ICANN Compliance's scope and remit." ● RrSG notes elements of concern about several individual recommendations in this grouping, as noted below: ● 9.1: "ICANN Contractual Compliance already performs this function through complaint processing, reviews, and audits. It is not clear to the RrSG what problem this recommendation is intended to fix". ● 9.2: "ICANN Compliance already proactively monitors compliance through audits and review, and additionally in light of complaint processing, does this". ● 9.3: "Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing". ● 9.4: "As part of ongoing collaboration between the RrSG and ICANN Contractual Compliance, the RrSG has requested ICANN Contractual Compliance make its needs for additional tools known to the RrSG on several occasions. The RrSG is not aware of any specific recommendations from ICANN Contractual Compliance".
Dependencies:	n/a

Considerations:	Not clear what would be audited, against what criteria, by whom (and why an external auditor would be required). In order for the Board to take dispositive action, ICANN org recommends further consultation with the SSR2 Implementation Shepherds on this recommendation to better understand the intent of the recommendation.
Possible clarifying questions:	● What "Compliance activities" does the SSR2 RT intend would be audited? ● What would be the scope of the audits? ● What standards would Compliance be audited against? ● What kinds of information would be requested that is not currently already published? ● Does the RT have an example of an external party that would be able to perform such audits?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 9.4	
Recommendation text:	ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4) This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	

Lead:	Compliance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations, although IPC specifically notes support for this grouping of recommendations. BC further believes this grouping of recommendations should be top priority and INTA and ALAC emphasize "strong support" for this grouping of recommendations. ● M3AAWG and GAC note support for this grouping of recommendations. GAC notes "it is particularly concerning that ICANN Contractual Compliance would assert to the SSR2 Review Team in April 2018 - that 'current contracts with registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus ineffective in allowing them to pursue those engaged in systemic DNS Abuse.' This gap in the current contracts, identified by both ICANN Contract Compliance and the ICANN Board demonstrates the need for improved and enforceable provisions to address DNS Abuse". ● While Article 19 agrees with the objective of this grouping of recommendations, it "strongly oppose[s]" the "proposition to develop and deploy monitoring systems without strong due process procedures in place, including the creation of a clear timeline to take action against the domain name after providing the registrant with opportunities to explain their action. We also oppose any attempts to include content takedowns without due process." Elements of concern: ● RySG believes Recommendation 9.1 specifically to be "extremely vague and we reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars. Such a recommendation exceeds the scope of this Review". ● RySG disagrees with the "implication" of this grouping of recommendations that "ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement", and notes that "Registry Operators' compliance with the abuse obligations were recently audited by ICANN Compliance". ● PIR makes an overarching comment to the SSR2 final report that some "recommendations imply that ICANN Compliance is not enforcing existing contractual obligations or encourage ICANN Compliance to undertake activities that are clearly outside of ICANN Compliance's scope and remit." ● RrSG notes elements of concern about several individual recommendations in this grouping, as noted below: ● 9.1: "ICANN Contractual Compliance already performs this function through complaint processing, reviews, and audits. It is not clear to the RrSG what problem this recommendation is intended to fix".

	● 9.2: “ICANN Compliance already proactively monitors compliance through audits and review, and additionally in light of complaint processing, does this”. ● 9.3: “Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing”. ● 9.4: “As part of ongoing collaboration between the RrSG and ICANN Contractual Compliance, the RrSG has requested ICANN Contractual Compliance make its needs for additional tools known to the RrSG on several occasions. The RrSG is not aware of any specific recommendations from ICANN Contractual Compliance”.
Dependencies:	n/a
Considerations:	ICANN org’s Contractual Compliance operations already in place ensure that registries and registrars fulfill the requirements in their agreements with ICANN org. Through the Contractual Compliance team, ICANN org enforces policies that have been adopted by the community and makes operational and structural changes as needed to carry out its enforcement role. ICANN org’s Contractual Compliance team cannot serve in a proactive policy development capacity. While the Board could support the idea of improving the tools that the ICANN org Contractual Compliance team has available to it in order to enforce policies that have been adopted by the community, the Board cannot approve the part of the recommendation that contemplates “measures that would require changes to the contracts” as such changes cannot be undertaken by either the Board or ICANN org unilaterally. These agreements are determined and agreed upon by the community. As such, this portion of the recommendation is not consistent with the role and authority of ICANN org’s Contractual Compliance team. The Board could encourage ICANN org’s Contractual Compliance team to continue pursuing new tools that will help improve its work.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject because the recommendation cannot be approved in full.

SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms

Recommendation 10.1	
Recommendation text:	ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct—ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (10.1 - 10.3) This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date. This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Policy / Gutsy Star
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC further highlights this grouping of recommendations as “top priority”, and ALAC indicates “strong support”. ● GAC, Tucows and M3AAWG note support for this grouping of recommendations as-is.

	• In general, commenters agree that clarity around terminology and definitions of DNS abuse is important.
	• RySG notes that "any discussion around a definition of DNS Abuse in the ICANN context must bear in mind ICANN's remit as outlined in the Bylaws. A resulting definition cannot exceed the Bylaws".
	• Article 19 suggests the "recommendation should be redrafted to ensure that the process proposed in the recommendation for coming up with a working definition of DNS abuse is only carried out after engaging in a multi-stakeholder process such as public comments or consultations that considers all positions on DNS abuse from across the ICANN Empowered Community".
	
	Elements of concern:
	• Namecheap believes this grouping of recommendations "will result in significant costs - without contemplating the impact on the limited ICANN budget", and as such recommends that the ICANN Board reject this grouping.
	• RrSG notes a position on individual recommendations in this grouping, as noted in the following excerpts:
	  ◦ 10.1: "It is not clear why the Review Team has made this recommendation. This recommendation implies that ICANN is not already doing all of the activities within the recommendation, whereas these activities are already ongoing".
	  ◦ 10.2: "The formation of a CCWG as described in this recommendation is outside of the ICANN Bylaws and the GNSO Operating Procedures. Additionally, the directions are overly prescriptive, do not allow for realistic timelines, and do not clearly state the problem that the recommendation is attempting to solve".

Dependencies:	• Dependencies on ongoing discussion regarding DNS abuse definition. • Could be considered dependent on SSR2 recommendation 10.2, output of the CCWG work on DNS abuse definition. • CCT recommendations 14 & 15 relate to DNS abuse definitions. Both of these recommendations are in 'pending' status. Board action (see the scorecard): "Place this recommendation in "Pending" status. The Board directs ICANN org to facilitate community efforts to develop a definition of "abuse" to inform further action on this recommendation. To negotiate amendments to address DNS Security Abuse measures, a common understanding of what "abuse" means must first be reached." • In its ICANN71 communique, the GAC encourages the Board to "facilitate work between the Board, ICANN Org, GNSO, GAC and other interested AC/SOs to ensure implementation to the extent possible of the following Recommendations with respect to existing gTLDs, and gTLDs introduced through any subsequent application process", including CCT recommendations 14 & 15.
Considerations:	• While this recommendation is grouped with 10.2 and 10.3, it could be considered separately from Recommendations 10.2 and 10.3.

	● GNSO Council "asks the ICANN Board to consider present and near-term demands of other policy work on the ICANN Org, staff, and larger ICANN community. Without a common and agreed upon definition, any additional policy work on a topic as broad as 'DNS abuse' would therefore appear extremely challenging and limiting the remit of any such policy related work ● ICANN org agrees with the value of documenting what it already does for more clarity and transparency of ICANN org's work on DNS security threat mitigation through its existing contractual and compliance mechanisms, and facilitates ongoing community discussions around definitions of DNS security threats. ● Considerations may be particularly important as definitions, procedures and protocols may evolve over time. It may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ICANN org's Information Transparency Initiative (ITI).
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 10.2	
Recommendation text:	Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (10.1 - 10.3) This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date. This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.

Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Policy / Gutsy Star

Summary of Public Comment:	Elements of support:
	● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC further highlights this grouping of recommendations as "top priority", and ALAC indicates "strong support".
	● GAC, Tucows and M3AAWG note support for this grouping of recommendations as-is.
	● In general, commenters agree that clarity around terminology and definitions of DNS abuse is important.
	● RySG notes that "any discussion around a definition of DNS Abuse in the ICANN context must bear in mind ICANN's remit as outlined in the Bylaws. A resulting definition cannot exceed the Bylaws".
	● Article 19 suggests the "recommendation should be redrafted to ensure that the process proposed in the recommendation for coming up with a working definition of DNS abuse is only carried out after engaging in a multi-stakeholder process such as public comments or consultations that considers all positions on DNS abuse from across the ICANN Empowered Community".
	
	Elements of concern:
	● Namecheap believes this grouping of recommendations "will result in significant costs - without contemplating the impact on the limited ICANN budget", and as such recommends that the ICANN Board reject this grouping.
	● RrSG notes a position on individual recommendations in this grouping, as noted in the following excerpts:
	  ● 10.1: "It is not clear why the Review Team has made this recommendation. This recommendation implies that ICANN is not already doing all of the activities within the recommendation, whereas these activities are already ongoing".
	  ● 10.2: "The formation of a CCWG as described in this recommendation is outside of the ICANN Bylaws and the GNSO Operating Procedures. Additionally, the directions are overly prescriptive, do not allow for realistic timelines, and do not clearly state the problem that the recommendation is attempting to solve".

Dependencies:	Dependent on community work for elements that are outside the remit of ICANN org or Board.

Considerations:	Seems to be asking for a CCWG for items that should be in the policy realm. ● GNSO Council "asks the ICANN Board to consider present and near-term demands of other policy work on the ICANN Org, staff, and larger ICANN community. Without a common and agreed upon definition, any additional policy work on a topic as broad as 'DNS abuse' would therefore appear extremely challenging and limiting the remit of any such policy related work. Niether ICANN org or Board can unilaterally establish a cross-community working group. A cross-community working group is a mechanism created by the community to facilitate collaborative work on topics that have been identified as not being within the remit of a specific Supporting Organization or Advisory Committee. Although there is no mandatory process governing the creation or operation of a CCWG, the ccNSO and GNSO communities developed a Uniform Framework for Principles & Recommendations for CCWGs in 2016 that clarifies the views of two of ICANN's policymaking bodies regarding the circumstances and scope for which a CCWG is appropriate. However, the community continues its discussions over DNS security threat mitigation. Discussions include questions around the definitions and scope of DNS security threats that can be considered as coming within ICANN's remit and the extent to which policy or other community work may be required to supplement efforts already underway, such as industry-led initiatives.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject because the recommendation cannot be approved in full.

Recommendation 10.3	
Recommendation text:	Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (10.1 - 10.3) This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date.

	This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Comms
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC further highlights this grouping of recommendations as "top priority", and ALAC indicates "strong support". ● GAC, Tucows and M3AAWG note support for this grouping of recommendations as-is. ● In general, commenters agree that clarity around terminology and definitions of DNS abuse is important. ● RySG notes that "any discussion around a definition of DNS Abuse in the ICANN context must bear in mind ICANN's remit as outlined in the Bylaws. A resulting definition cannot exceed the Bylaws". ● Article 19 suggests the "recommendation should be redrafted to ensure that the process proposed in the recommendation for coming up with a working definition of DNS abuse is only carried out after engaging in a multi-stakeholder process such as public comments or consultations that considers all positions on DNS abuse from across the ICANN Empowered Community". Elements of concern: ● Namecheap believes this grouping of recommendations "will result in significant costs - without contemplating the impact on the limited ICANN budget", and as such recommends that the ICANN Board reject this grouping. ● RrSG notes a position on individual recommendations in this grouping, as noted in the following excerpts: ● 10.1: "It is not clear why the Review Team has made this recommendation. This recommendation implies that ICANN is not already doing all of the activities within the recommendation, whereas these activities are already ongoing". ● 10.2: "The formation of a CCWG as described in this recommendation is outside of the ICANN Bylaws and the GNSO Operating Procedures.

	Additionally, the directions are overly prescriptive, do not allow for realistic timelines, and do not clearly state the problem that the recommendation is attempting to solve”.
Dependencies:	Dependent on implementation of SSR2 recommendation 10.2.
Considerations:	This recommendation is dependent on 10.2.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject because the recommendation cannot be approved in full.

SSR2 Recommendation 11: Resolve CZDS Data Access Problems

Recommendation 11.1	
Recommendation text:	The ICANN community and ICANN org should take steps to ensure that access to Centralized Zone Data Service (CZDS) data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 11: Resolve CZDS Data Access Problems (11.1) This recommendation can be considered implemented when ICANN org and the community makes access to CZDS data available in a timely manner and without unnecessary hurdles to requesters. This recommendation can be considered effective when ICANN org reports a decrease in the number of zone file access complaints and improves the ability for researchers to study the security-related operations of the DNS. This recommendation aims to establish proper access to the security-relevant zone file data used by academics and security specialists. This recommendation requires action from the ICANN Board, ICANN org, and the GNSO.
Owner (SSR2 assigned):	ICANN community and ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	GDS
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this recommendation. BC highlights this recommendation as “top priority”. ● M3AAWG supports this recommendation, as it believes “access to the CZDS remains problematic, particularly for researchers who use CZDS data longitudinally”. ● GAC supports improvements to processes “to the extent that access to such data as the Centralized Zone Data Service (CZDS) has been promised - but not realized”. Elements of concern: ● While it supports the recommendation as noted above, IPC notes checks and balances on access to CZDS data should be retained.

	• RySG believes the recommendation is "superfluous and out of scope", noting "the current system for access to CZDS data not only provides sufficient access but was also the result of lengthy negotiations taking into account the varying needs of different members of the ICANN community, including the registries that provide this access." • RySG notes the risk of "zone file data to be misused to disrupt legitimate business activities" and notes that "the current CZDS requirements reflect a balance between ease of access to zone file data, and responsible registry practices to ensure that requestors are accountable for their use of zone file data".
Dependencies:	n/a
Considerations:	In order for the Board to take dispositive action, ICANN org recommends that the Board consult with the SSR2 Implementation Shepherds on this recommendation to better understand the intent of the recommendation. ICANN org notes that in its 27 March 2020 public comments regarding this issue that the "Registry Agreement does not specify a timeframe in which registry operators must provide zone file access" and can only be changed "through a consensus policy development process or through voluntary contract negotiations." Additionally, ICANN org pointed out that the current CZDS system provides registry operators with an "auto-approve" option to "help expedite approval of access for those registry operators that wish to automate approvals for certain (or all) CZDS users." It is also worth noting that the Registries Stakeholder Group (RySG) believes this recommendation to be "superfluous and out of scope." The RySG further notes that the recommendation ignores the fact that the current CZDS system "not only provides sufficient access but was also the result of lengthy negotiations taking into account the varying needs of different members of the ICANN community, including the registries that provide this access." Additionally, Noncommercial Stakeholder Group (NCSG) calls this recommendation a "risky path" to "extending" ICANN org's mission.
Possible clarifying questions:	Based on this, ICANN org recommends that the following clarifying questions be sent to the Implementation Shepherds: • The Board notes that ICANN org is currently in the process of implementing recommendations from SAC097, which calls for ICANN org to revise "the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default. Can the SSR2 implementation shepherds provide further details as to what additional work is needed to sufficiently complete this recommendation and/or how the existing work being done on CZDS access is insufficient?
Proposed recommended Board action:	Pending, hold to seek clarity or further Information.

SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review

Recommendation 12.1	
Recommendation text:	ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review (12.1 - 12.4) This recommendation can be considered implemented when ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data. This recommendation can be considered effective when all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● In addition to their overarching support for the SSR2 recommendations, BC highlights this grouping of recommendations as "top priority", while ALAC emphasizes "strong support". ● M3AAWG supports this grouping of recommendations, agreeing that ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes. ● GAC notes that it supports "improving usability, transparency, and reproducibility of existing DNS Abuse Reporting", however it believes that this exercise may require nuance and compromise" and details several considerations to this point in its comments.

	• INTA notes the following excerpted points by way of support for the individual recommendations in this grouping, in addition to its overarching support for all SSR2 recommendations:
	  ◦ 12.1: "It is critical that DNS abuse mitigation and reporting activities within ICANN be conducted free of conflicts of interest and in an open and transparent manner to the extent possible without jeopardizing the effectiveness of such efforts".
	  ◦ 12.3: "While INTA supports incentives for registry operators and registrars who are proactive in combating abuse, it also supports publicly identifying registry operators and registrars who allow abusive domain names to persist and proliferate within their namespaces. ICANN Compliance must also use this data to impose meaningful consequences on registry operators and registrars who do not act in good faith to address abusive domain names."
	  ◦ 12.4: "Transparency with respect to anti-abuse activities will enable a better understanding of the landscape by all parties
	
	Elements of concern:
	• While Article 19 supports the grouping of recommendations, it notes that "any process of dealing with DNS abuse should be done through a public consultation process and should not expand ICANN's mandate beyond infrastructure to include content regulation".
	• RySG and RrSG believe that it is not clear what issue the recommendations are trying to address, given the work that is already underway. For example, RySG notes, "the RySG's DNS Abuse Working Group (and its predecessor the DAAR Working Group) has been working collaboratively with OCTO to ensure that DAAR provides the community with the best information available. Without a stated objective or observable problem this recommendation prescribes a solution with dubious value".
	• Tucows raises a specific concern that recommendation 12.3 is "attempting to identify registries and registrars that 'contribute to abuse' by quantifying the number of abusive registrations or clients on their platform instead simply indicates a high-volume business. Instead, attention should be given to business practices which allow for abusive behaviour or clients with indicators of abusive intent."
	• NCSG believes that "DAAR was never set up for the purpose of auditing registries and registrars...it should not be discontinued at the request of the review team but the community as a whole should decide which direction it should take".

Dependencies:	Extensive community work on DNS abuse.
Considerations:	Org suggests that the Board consider Recommendations 12.1 - 12.4 as a group. This grouping of recommendations along with other recommendations that pertain to DNS security threats will be considered in a coordinated way, including through the internal project dedicated to DNS security threats.

	• A better understanding of the RT's definition of "actionable data'' and "validation" is needed as well as understanding what information the RT believes is not transparent. We would need to better understand why the RT feels that the reporting can't be independently reproduced. • DNS Abuse is touched by many parts of the organization and efforts should be limited to only DNS Abuse reporting (via DAAR). • Significant contracting resources and complicated negotiations; loss of data as a whole if the vendor does not agree to share; potential use of ICANN resources beyond mission • Elements of this recommendation require clarification from the implementation shepherds, and would benefit from alignment with other work related to DNS security threats.
Possible clarifying questions:	• What is meant by "actionable data"? Actionable by whom and what constitutes an action?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 12.2	
Recommendation text:	ICANN org should structure its agreements with data providers to allow further sharing of the data for non-commercial use, specifically for validation or peer-reviewed scientific research. This special no-fee non-commercial license to use the data may involve a time-delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN website. ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review (12.1 - 12.4) This recommendation can be considered implemented when ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data. This recommendation can be considered effective when all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.
Owner (SSR2 assigned):	ICANN org

Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	OCTO

Summary of Public Comment:	Elements of support:
	● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations.
	● In addition to their overarching support for the SSR2 recommendations, BC highlights this grouping of recommendations as "top priority", while ALAC emphasizes "strong support".
	● M3AAWG supports this grouping of recommendations, agreeing that ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes.
	● GAC notes that it supports "improving usability, transparency, and reproducibility of existing DNS Abuse Reporting", however it believes that this exercise may require nuance and compromise" and details several considerations to this point in its comments.
	● INTA notes the following excerpted points by way of support for the individual recommendations in this grouping, in addition to its overarching support for all SSR2 recommendations:
	  ● 12.1: "It is critical that DNS abuse mitigation and reporting activities within ICANN be conducted free of conflicts of interest and in an open and transparent manner to the extent possible without jeopardizing the effectiveness of such efforts".
	  ● 12.3: "While INTA supports incentives for registry operators and registrars who are proactive in combating abuse, it also supports publicly identifying registry operators and registrars who allow abusive domain names to persist and proliferate within their namespaces. ICANN Compliance must also use this data to impose meaningful consequences on registry operators and registrars who do not act in good faith to address abusive domain names."
	  ● 12.4: "Transparency with respect to anti-abuse activities will enable a better understanding of the landscape by all parties
	
	Elements of concern:
	● While Article 19 supports the grouping of recommendations, it notes that "any process of dealing with DNS abuse should be done through a public consultation process and should not expand ICANN's mandate beyond infrastructure to include content regulation".
	● RySG and RrSG believe that it is not clear what issue the recommendations are trying to address, given the work that is already underway. For example, RySG notes, "the RySG's DNS Abuse Working Group (and its predecessor the DAAR Working Group) has been working collaboratively with OCTO to ensure that DAAR provides the community with the best information available.

	Without a stated objective or observable problem this recommendation prescribes a solution with dubious value". ● Tucows raises a specific concern that recommendation 12.3 is "attempting to identify registries and registrars that 'contribute to abuse' by quantifying the number of abusive registrations or clients on their platform instead simply indicates a high-volume business. Instead, attention should be given to business practices which allow for abusive behaviour or clients with indicators of abusive intent." ● NCSG believes that "DAAR was never set up for the purpose of auditing registries and registrars...it should not be discontinued at the request of the review team but the community as a whole should decide which direction it should take".
Dependencies:	Extensive community work on DNS abuse.
Considerations:	Org suggests that the Board consider Recommendations 12.1 - 12.4 as a group. This grouping of recommendations along with other recommendations that pertain to DNS abuse will be considered in a coordinated way, including through internal projects dedicated to DNS security threats. While it is unlikely that any reputation block list provider would agree to the terms, it's merely a question of negotiation. The org may want to clarify with the Implementation Shepherds what a successful implementation of this would be if we are unable to change the terms of the contracts with the data providers. Lots of diverse opinions on this and an underlying question of a successful implementation if the data providers are not willing to issue a license as described in the recommendation. It is not clear what independent verification means in this context .. do they mean those verifying should have the data for free? or that those verifying should be able to enter into their own contract with the data provider to gain the same data that the Org does? Significant contracting resources and complicated negotiations; loss of data as a whole if the vendor does not agree to share; potential use of ICANN resources beyond mission Elements of this recommendation require clarification from the implementation shepherds, and would benefit from alignment with other work related to DNS security threats.
Possible clarifying questions:	● What level of verification did the SSR2 RT intend? For example, does publication of the methodology meet the envisioned threshold? ● Can you provide specific examples of such a "no-fee non-commercial-licence", for reference? ● The recommendation states "ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting." Please clarify if this means verification of the data provider's methodology?

Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 12.3	
Recommendation text:	ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review (12.1 - 12.4) This recommendation can be considered implemented when ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data. This recommendation can be considered effective when all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● In addition to their overarching support for the SSR2 recommendations, BC highlights this grouping of recommendations as "top priority", while ALAC emphasizes "strong support". ● M3AAWG supports this grouping of recommendations, agreeing that ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes. ● GAC notes that it supports "improving usability, transparency, and reproducibility of existing DNS Abuse Reporting", however it believes that this exercise may require nuance and compromise" and details several considerations to this point in its comments.

	● INTA notes the following excerpted points by way of support for the individual recommendations in this grouping, in addition to its overarching support for all SSR2 recommendations:
	  ● 12.1: “It is critical that DNS abuse mitigation and reporting activities within ICANN be conducted free of conflicts of interest and in an open and transparent manner to the extent possible without jeopardizing the effectiveness of such efforts”.
	  ● 12.3: “While INTA supports incentives for registry operators and registrars who are proactive in combating abuse, it also supports publicly identifying registry operators and registrars who allow abusive domain names to persist and proliferate within their namespaces. ICANN Compliance must also use this data to impose meaningful consequences on registry operators and registrars who do not act in good faith to address abusive domain names.”
	  ● 12.4: “Transparency with respect to anti-abuse activities will enable a better understanding of the landscape by all parties
	
	Elements of concern:
	● While Article 19 supports the grouping of recommendations, it notes that “any process of dealing with DNS abuse should be done through a public consultation process and should not expand ICANN’s mandate beyond infrastructure to include content regulation”.
	● RySG and RrSG believe that it is not clear what issue the recommendations are trying to address, given the work that is already underway. For example, RySG notes, “the RySG’s DNS Abuse Working Group (and its predecessor the DAAR Working Group) has been working collaboratively with OCTO to ensure that DAAR provides the community with the best information available. Without a stated objective or observable problem this recommendation prescribes a solution with dubious value”.
	● Tucows raises a specific concern that recommendation 12.3 is “attempting to identify registries and registrars that ‘contribute to abuse’ by quantifying the number of abusive registrations or clients on their platform instead simply indicates a high-volume business. Instead, attention should be given to business practices which allow for abusive behaviour or clients with indicators of abusive intent.”
	● NCSG believes that “DAAR was never set up for the purpose of auditing registries and registrars...it should not be discontinued at the request of the review team but the community as a whole should decide which direction it should take”.

Dependencies:	Extensive community work on DNS abuse.
Considerations:	Org suggests that the Board consider Recommendations 12.1 - 12.4 as a group. This grouping of recommendations along with other recommendations that pertain to DNS abuse will be considered in a coordinated way, including through internal projects dedicated to DNS security threats.

	• Requires assessing risks associated with naming names and mitigating those risks as much as possible. • Naming names is already done by various other organizations (e.g.,Spamhaus). • Lots of diverse views on whether ICANN should publish data and at what level of granularity. The word "formats" suggests an open-ended model on how Org should publish (ie, text only, JSON, XML, etc..). Further clarity would be required before a recommended action to the board could take place • This is doable, but there are hurdles with the licensed data that the org subscribes to in order to reveal this data, as well as potentially creating legal liability issues for the org • Elements of this recommendation require clarification from the implementation shepherds, and would benefit from alignment with other work related to DNS security threats.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 12.4	
Recommendation text:	ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review (12.1 - 12.4) This recommendation can be considered implemented when ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data. This recommendation can be considered effective when all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.
Owner (SSR2 assigned):	ICANN org

Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	GDS

Summary of Public Comment:	Elements of support:
	● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations.
	● In addition to their overarching support for the SSR2 recommendations, BC highlights this grouping of recommendations as "top priority", while ALAC emphasizes "strong support".
	● M3AAWG supports this grouping of recommendations, agreeing that ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes.
	● GAC notes that it supports "improving usability, transparency, and reproducibility of existing DNS Abuse Reporting", however it believes that this exercise may require nuance and compromise" and details several considerations to this point in its comments.
	● INTA notes the following excerpted points by way of support for the individual recommendations in this grouping, in addition to its overarching support for all SSR2 recommendations:
	  ● 12.1: "It is critical that DNS abuse mitigation and reporting activities within ICANN be conducted free of conflicts of interest and in an open and transparent manner to the extent possible without jeopardizing the effectiveness of such efforts".
	  ● 12.3: "While INTA supports incentives for registry operators and registrars who are proactive in combating abuse, it also supports publicly identifying registry operators and registrars who allow abusive domain names to persist and proliferate within their namespaces. ICANN Compliance must also use this data to impose meaningful consequences on registry operators and registrars who do not act in good faith to address abusive domain names."
	  ● 12.4: "Transparency with respect to anti-abuse activities will enable a better understanding of the landscape by all parties
	
	Elements of concern:
	● While Article 19 supports the grouping of recommendations, it notes that "any process of dealing with DNS abuse should be done through a public consultation process and should not expand ICANN's mandate beyond infrastructure to include content regulation".
	● RySG and RrSG believe that it is not clear what issue the recommendations are trying to address, given the work that is already underway. For example, RySG notes, "the RySG's DNS Abuse Working Group (and its predecessor the DAAR Working Group) has been working collaboratively with OCTO to ensure that DAAR provides the community with the best information available. Without a

	stated objective or observable problem this recommendation prescribes a solution with dubious value". ● Tucows raises a specific concern that recommendation 12.3 is "attempting to identify registries and registrars that 'contribute to abuse' by quantifying the number of abusive registrations or clients on their platform instead simply indicates a high-volume business. Instead, attention should be given to business practices which allow for abusive behaviour or clients with indicators of abusive intent." ● NCSG believes that "DAAR was never set up for the purpose of auditing registries and registrars...it should not be discontinued at the request of the review team but the community as a whole should decide which direction it should take".
Dependencies:	Extensive community work on DNS abuse.
Considerations:	Org suggests that the Board consider Recommendations 12.1 - 12.4 as a group. This grouping of recommendations along with other recommendations that pertain to DNS abuse will be considered in a coordinated way, including through internal projects dedicated to DNS security threats. SSR2 Recommendation 12.4 overlaps with CCT recommendation 20, which calls for ICANN org to determine "what actions registries have taken to respond to complaints of illegal or malicious conduct in connection with the use of the TLD." In its 22 October 2020 resolution on CCT Recommendation 20 (among others), the Board noted that "under the current terms of ICANN's agreements with contracted parties, ICANN org does not have the authority to demand information that registries are not required to collect or submit to ICANN org." However, ICANN org provided analysis in its Detailed Assessment of the CCT Recommendations that showed the information could be collected via a voluntary survey (in consultation with contracted parties). Accordingly, the Board approved CCT Recommendation 20 and directed ICANN org to conduct a pilot voluntary survey. Elements of this recommendation require clarification from the implementation shepherds, and would benefit from alignment with other work related to DNS security threats.
Possible clarifying questions:	● Please clarify the SSR2 RT's expectations for the recommended reports. For example, would the report provide information regarding the number of domains suspended in a year by a contracted party and whether the domains were suspended in response to legal obligations or voluntarily? ● Please clarify what the SSR2 RT means by "voluntary" actions, and whether, for example, any action taken that is not in response to a Law Enforcement Agency would be considered voluntary?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting

Recommendation 13.1	
Recommendation text:	ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all generic top-level domains (gTLDs); the participation of each country code top-level domain (ccTLD) would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting (13.1 - 13.2) This recommendation can be considered implemented when ICANN org simplifies the process of submitting and receiving abuse complaints and offers insight into the number of complaints and some metadata (e.g., type of abuse reported, dates, time to resolution) for researchers and community members. This recommendation can be considered complete when the portal is up and running. This recommendation can be considered effective when contracted parties have to spend less time on misdirected complaints, and the research community as well as the broader ICANN community can see and study the associated data about those complaints. Due to the complexity of this enterprise, this recommendation is expected to take several years (at least three) after the ICANN Board approves the implementation of this recommendation.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	GDS
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC highlights this grouping of recommendations as “top priority”, and ALAC notes “strong support”. ● M3AAWG notes support for this grouping of recommendations.

	• Article 19 welcomes the recommendation but suggests "reviewing the data collection process to ensure that only the necessary and minimum available data (excluding personally identifiable information) is collected prior to increasing transparency and accountability of this data". • GAC "strongly supports the creation of a centralized DNS Abuse complaint portal capable of automatically routing all abuse reporting to the relevant parties", however "is agnostic as to the party operating such a complaint portal". Elements of concern: • RySG has "concerns about the quality of the proposed output... Any such reporting system would need to include a process to qualify the accuracy and legitimacy of the complaints submitted before they are passed on for required action by Contracted Parties or aggregated and published in a report". • Namecheap notes several concerns with this grouping of recommendations, however it notes that the "biggest concern" is cost. Namecheap believes the recommendation should be rejected due to the "significant costs to ICANN". • RrSG believes that the Board should reject the recommendations in this grouping based on RrSG's concerns that it is not clear what the recommendations are attempting to achieve or how they will be funded. • Further, RrSG notes concerns that the proposed system could be subject to abuse, a concern it believes the SSR2 Review Team has not identified or addressed.
Dependencies:	Extensive community work on DNS abuse.
Considerations:	Building such a system would be very complex. Note that this system would not involve any enforcement activity and is unrelated to Compliance function. In addition, there is no contractual requirement for contracted parties to use this system. Requires contractual changes, otherwise it would be purely voluntary. ICANN org suggests that the Board consider Recommendations 13.1 and 13.2 together with Recommendations 12.1 - 12.4. This grouping of recommendations along with other recommendations that pertain to DNS security threats will be considered in a coordinated way, including through the internal project dedicated to DNS security threats. SSAC offers an alternative view to this recommendation in SAC115. In order for the Board to take dispositive action, ICANN org recommends that the Board consult with the SSR2 Implementation Shepherds on this recommendation to better understand the intent of the recommendation. It is also worth noting that the Registries Stakeholder Group (RySG) and the Registrars Stakeholder Group (RrSG) both have apprehensions regarding this recommendation:

	• The RySG notes that they have “serious concerns” about the quality of data produced from the proposed reporting system, which would further require the development of a “process to qualify the accuracy and legitimacy of the complaints” before the data could be passed to contracted parties or published in a report. • The RrSG calls for this recommendation to be rejected as it “is not clear what this recommendation is attempting to accomplish.” Due to the complexity of this enterprise, this recommendation is expected to take several years (at least three) after the ICANN Board approves the implementation of this recommendation.
Possible clarifying questions:	ICANN org recommends the following clarifying question be sent to the Implementation Shepherds: • Can the SSR2 Implementation Shepherds provide additional details as to what issues the SSR2 intended for this recommendation to solve? ICANN org notes that abuse reports are typically submitted by RDDS end-users and there are existing processes for submitting complaints. • Can the SSR2 Implementation Shepherds clarify its recommendation that “use of the system should become mandatory”? ICANN org notes that only through consensus policies or agreements can particular actions become mandatory, not unilaterally through the ICANN Board or org. • Can the SSR2 Implementation Shepherds provide additional details as to whether the SSR2 Review Team considered how and by whom complaints would be vetted? • Please clarify what is expected of "gTLDs" in the use of a "central DNS abuse complaint portal"? Typically, abuse reports are submitted by RDDS end-users. • Did the SSR2 RT undertake an assessment of risks to ICANN org should gTLDs reject the mandatory recommendation?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 13.2	
Recommendation text:	ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting (13.1 - 13.2) This recommendation can be considered implemented when ICANN org simplifies the process of submitting and receiving abuse complaints and offers insight into the

	number of complaints and some metadata (e.g., type of abuse reported, dates, time to resolution) for researchers and community members. This recommendation can be considered complete when the portal is up and running. This recommendation can be considered effective when contracted parties have to spend less time on misdirected complaints, and the research community as well as the broader ICANN community can see and study the associated data about those complaints. Due to the complexity of this enterprise, this recommendation is expected to take several years (at least three) after the ICANN Board approves the implementation of this recommendation.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Compliance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. BC highlights this grouping of recommendations as "top priority", and ALAC notes "strong support". ● M3AAWG notes support for this grouping of recommendations. ● Article 19 welcomes the recommendation but suggests "reviewing the data collection process to ensure that only the necessary and minimum available data (excluding personally identifiable information) is collected prior to increasing transparency and accountability of this data". ● GAC "strongly supports the creation of a centralized DNS Abuse complaint portal capable of automatically routing all abuse reporting to the relevant parties", however "is agnostic as to the party operating such a complaint portal". Elements of concern: ● RySG has "concerns about the quality of the proposed output... Any such reporting system would need to include a process to qualify the accuracy and legitimacy of the complaints submitted before they are passed on for required action by Contracted Parties or aggregated and published in a report". ● Namecheap notes several concerns with this grouping of recommendations, however it notes that the "biggest concern" is cost. Namecheap believes the recommendation should be rejected due to the "significant costs to ICANN".

	• RrSG believes that the Board should reject the recommendations in this grouping based on RrSG's concerns that it is not clear what the recommendations are attempting to achieve or how they will be funded. • Further, RrSG notes concerns that the proposed system could be subject to abuse, a concern it believes the SSR2 Review Team has not identified or addressed.
Dependencies:	Extensive community work on DNS abuse. Dependent on implementation of SSR2 recommendation 13.1.
Considerations:	ICANN org suggests that the Board consider Recommendations 13.1 and 13.2 together with Recommendations 12.1 - 12.4. This grouping of recommendations along with other recommendations that pertain to DNS security threats will be considered in a coordinated way, including through the internal project dedicated to DNS security threats. ICANN org already publishes this data, may not be not in the form that the "independent third party" wants. Seek clarification from shepherds as to what form of data SSR2 is required beyond what is already in place.
Possible clarifying questions:	• Please clarify what form of data is required besides the data that is currently published by ICANN Compliance? (see [LINK] to metrics)
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements

Recommendation 14.1	
Recommendation text:	ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2) SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Legal / Policy
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, BC suggests the grouping should be “top priority”, and ALAC emphasizes “strong support”.

	● GAC does not offer a view on "whether or not a Temporary Specification is necessary to accomplish the goals set forth in Recommendation 14", but "stresses the importance of urgent action on those security improvements-related recommendations".
	● M3AAWG supports this grouping of recommendations.
	● Regarding 14.5, RrSG notes: "While the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed. This includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN."
	
	Elements of concern:
	● Tucows "supports SSR2's commitment to evidence-based improvements but is not clear on why a Temporary Specification is recommended rather than a standard PDP...Any policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context".
	● RySG believes that "this grouping fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways: (1) The Recommendation fails to meet the requirement that a temporary specification be as 'narrowly tailored' as feasible to achieve its defined purposes; and (2) Temporary Specifications must address an immediate need to preserve the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues".
	● RrSG notes concerns about individual recommendations, as noted below:
	  ● 14.1: "The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA".
	  ● 14.2: "The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse".
	  ● 14.3: "In addition to recommending that the ICANN Board reject this recommendation, the RrSG is concerned that the Review Team recommends reviewing the veracity of data leading to abuse reports (that could ultimately lead to RAA or RA termination) AFTER the reports have been sent to the contracted party. Additionally, ICANN Contractual Compliance already has a robust abuse complaint process, so it is not clear why an additional process and system is required."
	  ● 14.4: "[this recommendation] ignores the ICANN multistakeholder approach, existing ICANN Compliance processes, and it is not proper to use a Review Team to create such overbearing restrictions on contracted parties".
	● PIR believes that this grouping of recommendations "violates the terms of the Registry Agreement that govern how temporary policies/specifications may be utilized by ICANN. In addition, the terms Stability and Security are not

	amorphous or generic concepts in the Registry Agreement, but rather are defined terms". ● Namecheap believes "the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine how to pay for the recommendation".
Dependencies:	Dependent on outcomes of CCT recommendations 12 and 14.
Considerations:	SSR2 Recommendations 14 and 15 are addressed together within the SSR2 Final Report. Temporary Policies can only be established by the ICANN Board and must meet specific requirements, viz. the Board "reasonably determines that such modifications or amendments are 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, the DNS or the Internet"[2,3]. ● GNSO Council does not offer a view on this grouping of recommendations but with regard to Recommendation 14.1 "asks the ICANN Board to consider present and near-term demands of other policy work on the ICANN Org, staff, and larger ICANN community". The Board, consistent with its action on the Competition, Consumer Trust, and Consumer Choice (CCT) recommendations, should not take the place of the community within the multistakeholder model and initiate a PDP upon a Specific Review team's recommendation.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject.

Recommendation 14.2	
Recommendation text:	To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for

[2] Base Registry Agreement - Updated 31 July 2017. Section 2: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf
[3] 2013 Registrar Accreditation Agreement 'Consensus Policies and Temporary Policies Specification':https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary

	blocklisting domains.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2) SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	GDS
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, BC suggests the grouping should be “top priority”, and ALAC emphasizes “strong support”. ● GAC does not offer a view on “whether or not a Temporary Specification is necessary to accomplish the goals set forth in Recommendation 14”, but “stresses the importance of urgent action on those security improvements-related recommendations”. ● M3AAWG supports this grouping of recommendations. ● Regarding 14.5, RrSG notes: “While the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed.

	This includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN." Elements of concern: ● Tucows "supports SSR2's commitment to evidence-based improvements but is not clear on why a Temporary Specification is recommended rather than a standard PDP...Any policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context". ● RySG believes that "this grouping fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways: (1) The Recommendation fails to meet the requirement that a temporary specification be as 'narrowly tailored' as feasible to achieve its defined purposes; and (2) Temporary Specifications must address an immediate need to preserve the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues". ● RrSG notes concerns about individual recommendations, as noted below: ● 14.1: "The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA". ● 14.2: "The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse". ● 14.3: "In addition to recommending that the ICANN Board reject this recommendation, the RrSG is concerned that the Review Team recommends reviewing the veracity of data leading to abuse reports (that could ultimately lead to RAA or RA termination) AFTER the reports have been sent to the contracted party. Additionally, ICANN Contractual Compliance already has a robust abuse complaint process, so it is not clear why an additional process and system is required." ● 14.4: "[this recommendation] ignores the ICANN multistakeholder approach, existing ICANN Compliance processes, and it is not proper to use a Review Team to create such overbearing restrictions on contracted parties". ● PIR believes that this grouping of recommendations "violates the terms of the Registry Agreement that govern how temporary policies/specifications may be utilized by ICANN. In addition, the terms Stability and Security are not amorphous or generic concepts in the Registry Agreement, but rather are defined terms". ● Namecheap believes "the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine how to pay for the recommendation".

Dependencies:	SSR2 recommendation 12.2.
Considerations:	ICANN org currently measures specific security threats related to domain names through several projects, including the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project, and Domain Abuse Activity Reporting System (DAAR), both of which have a publication or reporting element. All such projects rely on commercially licensed data that come with varying restrictions on what data can be shared and how. Through the Domain Name Security Threat Information Collection and Reporting (DNSTICR), ICANN org produces reports on recent domain registrations that ICANN org understands to be using the COVID-19 pandemic for phishing or malware campaigns. These reports, which are shared with the responsible parties (primarily registrars or registries), contain the evidence that leads ICANN org to believe the domains are being used maliciously, along with other background information to help the responsible parties determine the correct course of action. The overarching purpose of ICANN's Domain Abuse Activity Reporting System (DAAR) is to develop a robust, reliable, and reproducible methodology for analyzing security threat activity, which the ICANN community may use to make informed policy decisions. The system collects TLD zone data and complements these data sets with a large set of high-confidence Reputation Block List (RBL) security threat data feeds. The aggregated statistics and anonymized data collected by the DAAR system can serve as a platform for studying, reporting daily, or historically the registration data, or the abuse activity by each registry. This aggregated data is currently pushed to the registries using ICANN's Service Level Agreement Monitoring (SLAM) system. This recommendation, along with other recommendations that pertain to DNS security threats should be considered in a coordinated way, including through ICANN org's internal project dedicated to DNS security threats and ongoing projects such as DNSTICR and DAAR. Elements of this recommendation require clarification from the implementation shepherds, and would benefit from alignment with other work related to DNS security threats. It is also worth noting that the Registries Stakeholder Group (RySG) and the Registrars Stakeholder Group (RrSG) have differing opinions on this recommendation. The RySG notes that it is a "sensible recommendation" and could be a "valuable tool" in identifying abuse. The RrSG, however, calls for the Board to reject this recommendation as it is "not within ICANN's remit to police the Internet for abuse."
Possible clarifying questions:	The Board may wish to consult with the Implementation Shepherds regarding recommendation 14.2.

	ICANN org recommends the following clarifying questions be sent to the Implementation Shepherds: ● Can the Implementation Shepherds provide details as to expectations for the contracted parties in terms of actions to be taken on the lists provided by ICANN org?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 14.3	
Recommendation text:	Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and then issue a notice to the relevant party.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2) SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High

ICANN org assessment:	
Lead:	Compliance

Summary of Public Comment:	Elements of support:
	● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, BC suggests the grouping should be "top priority", and ALAC emphasizes "strong support".
	● GAC does not offer a view on "whether or not a Temporary Specification is necessary to accomplish the goals set forth in Recommendation 14", but "stresses the importance of urgent action on those security improvements-related recommendations".
	● M3AAWG supports this grouping of recommendations.
	● Regarding 14.5, RrSG notes: "While the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed. This includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN."
	
	Elements of concern:
	● Tucows "supports SSR2's commitment to evidence-based improvements but is not clear on why a Temporary Specification is recommended rather than a standard PDP...Any policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context".
	● RySG believes that "this grouping fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways: (1) The Recommendation fails to meet the requirement that a temporary specification be as 'narrowly tailored' as feasible to achieve its defined purposes; and (2) Temporary Specifications must address an immediate need to preserve the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues".
	● RrSG notes concerns about individual recommendations, as noted below:
	  ● 14.1: "The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA".
	  ● 14.2: "The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse".
	  ● 14.3: "In addition to recommending that the ICANN Board reject this recommendation, the RrSG is concerned that the Review Team recommends reviewing the veracity of data leading to abuse reports (that could ultimately lead to RAA or RA termination) AFTER the reports have been sent to the contracted party. Additionally, ICANN

	Contractual Compliance already has a robust abuse complaint process, so it is not clear why an additional process and system is required." ● 14.4: "[this recommendation] ignores the ICANN multistakeholder approach, existing ICANN Compliance processes, and it is not proper to use a Review Team to create such overbearing restrictions on contracted parties". ● PIR believes that this grouping of recommendations "violates the terms of the Registry Agreement that govern how temporary policies/specifications may be utilized by ICANN. In addition, the terms Stability and Security are not amorphous or generic concepts in the Registry Agreement, but rather are defined terms". ● Namecheap believes "the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine how to pay for the recommendation".
Dependencies:	Dependent on implementation of SSR2 recommendation 14.1.
Considerations:	SSR2 Recommendations 14 and 15 are addressed together within the SSR2 Final Report. Temporary Policies can only be established by the ICANN Board and must meet specific requirements, viz. the Board "reasonably determines that such modifications or amendments are 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, the DNS or the Internet"[4,5].
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject.

Recommendation 14.4	
Recommendation text:	ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Contractual Compliance should move to the de-accreditation process.

[4] Base Registry Agreement - Updated 31 July 2017. Section 2: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf
[5] 2013 Registrar Accreditation Agreement 'Consensus Policies and Temporary Policies Specification':https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary

SSR2-defined measures of success:	Applies to SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2) SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Compliance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, BC suggests the grouping should be “top priority”, and ALAC emphasizes “strong support”. ● GAC does not offer a view on “whether or not a Temporary Specification is necessary to accomplish the goals set forth in Recommendation 14”, but “stresses the importance of urgent action on those security improvements-related recommendations”. ● M3AAWG supports this grouping of recommendations. ● Regarding 14.5, RrSG notes: “While the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed. This includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN.”

	Elements of concern: ● Tucows "supports SSR2's commitment to evidence-based improvements but is not clear on why a Temporary Specification is recommended rather than a standard PDP...Any policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context". ● RySG believes that "this grouping fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways: (1) The Recommendation fails to meet the requirement that a temporary specification be as 'narrowly tailored' as feasible to achieve its defined purposes; and (2) Temporary Specifications must address an immediate need to preserve the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues". ● RrSG notes concerns about individual recommendations, as noted below: ● 14.1: "The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA". ● 14.2: "The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse". ● 14.3: "In addition to recommending that the ICANN Board reject this recommendation, the RrSG is concerned that the Review Team recommends reviewing the veracity of data leading to abuse reports (that could ultimately lead to RAA or RA termination) AFTER the reports have been sent to the contracted party. Additionally, ICANN Contractual Compliance already has a robust abuse complaint process, so it is not clear why an additional process and system is required." ● 14.4: "[this recommendation] ignores the ICANN multistakeholder approach, existing ICANN Compliance processes, and it is not proper to use a Review Team to create such overbearing restrictions on contracted parties". ● PIR believes that this grouping of recommendations "violates the terms of the Registry Agreement that govern how temporary policies/specifications may be utilized by ICANN. In addition, the terms Stability and Security are not amorphous or generic concepts in the Registry Agreement, but rather are defined terms". ● Namecheap believes "the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine
Dependencies:	Dependent on implementation of SSR2 recommendation 14.1.
Considerations:	Temporary Policies can only be established by the ICANN Board and must meet specific requirements, viz. the Board "reasonably determines that such modifications or amendments are 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, the DNS or the Internet"[6,7].
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject.

Recommendation 14.5	
Recommendation text:	ICANN org should consider offering financial incentives: contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2) SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.
Owner (SSR2 assigned):	ICANN org

[6] Base Registry Agreement - Updated 31 July 2017. Section 2: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf
[7] 2013 Registrar Accreditation Agreement 'Consensus Policies and Temporary Policies Specification':https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary

Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	GDS

Summary of Public Comment:	Elements of support:
	● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, BC suggests the grouping should be "top priority", and ALAC emphasizes "strong support".
	● GAC does not offer a view on "whether or not a Temporary Specification is necessary to accomplish the goals set forth in Recommendation 14", but "stresses the importance of urgent action on those security improvements-related recommendations".
	● M3AAWG supports this grouping of recommendations.
	● Regarding 14.5, RrSG notes: "While the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed. This includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN."
	
	Elements of concern:
	● Tucows "supports SSR2's commitment to evidence-based improvements but is not clear on why a Temporary Specification is recommended rather than a standard PDP...Any policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context".
	● RySG believes that "this grouping fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways: (1) The Recommendation fails to meet the requirement that a temporary specification be as 'narrowly tailored' as feasible to achieve its defined purposes; and (2) Temporary Specifications must address an immediate need to preserve the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues".
	● RrSG notes concerns about individual recommendations, as noted below:
	  ● 14.1: "The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA".
	  ● 14.2: "The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse".
	  ● 14.3: "In addition to recommending that the ICANN Board reject this recommendation, the RrSG is concerned that the Review Team recommends reviewing the veracity of data leading to abuse reports

	(that could ultimately lead to RAA or RA termination) AFTER the reports have been sent to the contracted party. Additionally, ICANN Contractual Compliance already has a robust abuse complaint process, so it is not clear why an additional process and system is required." ● 14.4: "[this recommendation] ignores the ICANN multistakeholder approach, existing ICANN Compliance processes, and it is not proper to use a Review Team to create such overbearing restrictions on contracted parties". ● PIR believes that this grouping of recommendations "violates the terms of the Registry Agreement that govern how temporary policies/specifications may be utilized by ICANN. In addition, the terms Stability and Security are not amorphous or generic concepts in the Registry Agreement, but rather are defined terms". ● Namecheap believes "the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine how to pay for the recommendation".
Dependencies:	Dependent on outcomes of CCT recommendations 12 and 14
Considerations:	SSR2 Recommendations 14 and 15 are addressed together within the SSR2 Final Report. SSR2 Recommendation 14.5 overlaps with CCT Recommendations 12 and 14, both of which call for the use of financial incentives for contracted parties. The Board passed CCT Recommendation 12 through to the New gTLD Subsequent Procedures Working Group (SubPro) and CCT Recommendation 14 is still pending action by the Board. In the "Detailed Assessment" provided by ICANN org in support of the Board's 22 October 2020 resolution, ICANN org noted that CCT Recommendation 14 is pending further community discussion and alignment on the definition of abuse. ICANN org also noted that it "is not in a position to provide an anticipated completion date for this action given the dependency on the community's agreement on what does, and does not, constitute "abuse" as well as possible next steps for any policy or other community work on this topic." In light of this, the Board may wish to seek clarification from the Implementation Shepherds as to how the SSR2 Review Team may have considered the CCT Recommendations in formulating SSR2 Recommendation 14.5. It should also be noted that the Board and org cannot unilaterally "offer financial incentives." Such a change would require changes to agreements with the contracted parties; changes which could only come about either through contract negotiations or policy development. Likewise, ICANN org noted in its comment on the SSR2 Initial Report concerns regarding offering incentives as this could lead to gaming. Finally, the RySG and RrSG again differ in their view of this recommendation. The RySG calls for SSR2 Recommendation 14.5 to be rejected (along with 14.1, 14.3, and 14.4). The RrSG states in contrast that "[w]hile the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed. This

	includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN." The Board may also wish to consult with the wider community, including contracted parties, as to how to address SSR2 Recommendation 14.5 in light of ongoing discussions regarding DNS Abuse in the community. - In its ICANN71 communique, the GAC encourages the Board to "facilitate work between the Board, ICANN Org, GNSO, GAC and other interested AC/SOs to ensure implementation to the extent possible of the following Recommendations with respect to existing gTLDs, and gTLDs introduced through any subsequent application process", including CCT recommendations 12 & 14. Temporary Policies can only be established by the ICANN Board and must meet specific requirements, viz. the Board "reasonably determines that such modifications or amendments are 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, the DNS or the Internet"[8,9].
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject.

[8] Base Registry Agreement - Updated 31 July 2017. Section 2: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

[9] 2013 Registrar Accreditation Agreement 'Consensus Policies and Temporary Policies Specification':https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary

SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements

Recommendation 15.1	
Recommendation text:	After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported Expedited Policy Development Process (EPDP) to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2) SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Policy
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations.

	Further, BC suggests the grouping should be “top priority”, and ALAC emphasizes “strong support”. ● M3AAWG notes support for this grouping of recommendations. ● GAC “supports Recommendation 15 to develop an EPDP on anti-abuse policy and in particular of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Contractual Compliance enforcement actions in case of policy violations. In line with this Recommendation, the GAC stresses the importance for ICANN org to insist on the power to terminate contracts in the case of a pattern and practice of harboring or ignoring abuse by any Contracted Party.” Elements of concern: ● RySG, PIR, Tucows, and RrSG believe that this grouping of recommendations does not meet the requirements for an EPDP. For example, RrSG states: “There is no need for an EPDP regarding abuse. The only difference between a PDP and an EPDP is that an EPDP does not have an issues report. Otherwise, an EPDP does not operate ‘faster’ than a normal PDP. As the RrSG disputes that any PDP regarding abuse is necessary (because no issues to be resolved have been clearly and articulately identified, as well as defined goals), it is imperative than any abuse PDP start with an issues report, and only then can the GNSO Council determine whether a full PDP is necessary to address the specific issues”. ● Further, the RrSG believes the proposals in recommendation 15.2 are “outside of ICANN’s remit” as “the community does not get to define how contracted parties operate. That is subject to negotiation between ICANN and the contracted parties, and limited to within ICANN remit.”
Dependencies:	Could be dependent on implementation of SSR2 recommendation 14.
Considerations:	SSR2 Recommendations 14 and 15 are addressed together within the SSR2 Final Report. ICANN’s policy development process is prescribed by the Bylaws and other documented procedures (e.g. the GNSO’s operating procedures).These processes ascribe to the GNSO Council the role and authority to initiate an EPDP. ● GNSO Council does not offer a view on this grouping of recommendations but with regard to Recommendation 15.1 “asks the ICANN Board to consider present and near-term demands of other policy work on the ICANN Org, staff, and larger ICANN community”. GNSO Council is the only one that can launch an EPDP. The Board can request an Issue Report and require the initiation of a PDP in the GNSO, an EPDP can only be launched by a GNSO Council vote, and only in specific circumstances (“to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the ICANN Board or the implementation of such an adopted recommendation; [or] to provide new or additional policy

	recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists"[10].) The Board notes that Recommendation 15.1 does not meet these requirements. As with CCT recommendations, ICANN org proposes that the Board does not use Specific Review team's recommendations as a basis for initiating policy development, and would instead defer to the community
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject.

Recommendation 15.2	
Recommendation text:	The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Contractual Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2) SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS

[10] GNSO Operating Rules and Procedures: Annex 4 - Expedited Policy Development Process Manual: https://gnso.icann.org/sites/default/files/file/field-file-attach/2016-12/annex-4-epdp-manual-01sep16-en.pdf

	abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	High
ICANN org assessment:	
Lead:	Policy
Summary of Public Comment:	Elements of concern: ● RySG, PIR, Tucows, and RrSG believe that this grouping of recommendations does not meet the requirements for an EPDP. For example, RrSG states: "There is no need for an EPDP regarding abuse. The only difference between a PDP and an EPDP is that an EPDP does not have an issues report. Otherwise, an EPDP does not operate 'faster' than a normal PDP. As the RrSG disputes that any PDP regarding abuse is necessary (because no issues to be resolved have been clearly and articulately identified, as well as defined goals), it is imperative than any abuse PDP start with an issues report, and only then can the GNSO Council determine whether a full PDP is necessary to address the specific issues". ● Further, the RrSG believes the proposals in recommendation 15.2 are "outside of ICANN's remit" as "the community does not get to define how contracted parties operate. That is subject to negotiation between ICANN and the contracted parties, and limited to within ICANN remit."
Dependencies:	Dependent on SSR2 recommendation 15.1.
Considerations:	SSR2 Recommendations 14 and 15 are addressed together within the SSR2 Final Report. ICANN's policy development process is prescribed by the Bylaws and other documented procedures (e.g. the GNSO's operating procedures).These processes ascribe to the GNSO Council the role and authority to initiate an EPDP. GNSO Council is the only one that can launch an EPDP. The Board can request an Issue Report and require the initiation of a PDP in the GNSO, an EPDP can only be launched by a GNSO Council vote, and only in specific circumstances ("to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the ICANN Board or the implementation of

	such an adopted recommendation; [or] to provide new or additional policy recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists"[11].) The Board notes that Recommendation 15.1 does not meet these requirements. As with CCT recommendations, ICANN org proposes that the Board does not use Specific Review team's recommendations as a basis for initiating policy development, and would instead defer to the community
Possible clarifying questions:	n/a
Proposed recommended Board action:	Reject.

[11] GNSO Operating Rules and Procedures: Annex 4 - Expedited Policy Development Process Manual: https://gnso.icann.org/sites/default/files/file/field-file-attach/2016-12/annex-4-epdp-manual-01sep16-en.pdf

SSR2 Recommendation 16: Privacy Requirements and RDS

Recommendation 16.1	
Recommendation text:	ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the Registration Directory Service (RDS).
SSR2-defined measures of success:	Applies to SSR2 Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3) This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	Comms
Summary of Public Comment:	Elements of support: By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC emphasizes "strong support". ● GAC suggests this grouping of recommendations "should specify clearly the need for balancing GDPR-type privacy considerations with the need to ensure access to non-personal data in line with the efforts under EPDP phase 2.A to ensure appropriate access to WHOIS registration data." Elements of concern: ● RySG is concerned that this grouping of recommendations "is not tied to a specific problem statement". ● RySG and RrSG believe that Recommendation 16.3 exceeds the scope of ICANN Complaince's role, as does RrSG. ● In addition to the above-noted concerns about Recommendation 16.3, RrSG notes the following concerns:

	● 16.1: “This recommendation attempts to override an existing ICANN initiative (ITI). As the ITI has been in process for a number of years, and is currently focusing on high volume and high priority items, the ITI should be allowed to continue its existing timeline as the Review Team has not provided any rationale for why RDS data should be prioritized over other action items in the ITI”. ● 16.2: “The ICANN Community should not be able to dictate the composition, scope, and function of ICANN Contractual Compliance”.
Dependencies:	Ongoing work on ITI project.
Considerations:	While the recommendation itself can be approved, it cannot override the ITI/IPT roadmap that is already in place. Once this has been more thoroughly scoped and the requirements are gathered, a timeline and approach can be confirmed.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 16.2	
Recommendation text:	ICANN org should create specialized groups within the Contractual Compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems).
SSR2-defined measures of success:	Applies to SSR2 Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3) This recommendation can be considered implemented when ICANN org’s actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.
Owner (SSR2 assigned):	ICANN org

Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	Compliance
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC emphasizes "strong support". ● GAC suggests this grouping of recommendations "should specify clearly the need for balancing GDPR-type privacy considerations with the need to ensure access to non-personal data in line with the efforts under EPDP phase 2.A to ensure appropriate access to WHOIS registration data." Elements of concern: ● RySG is concerned that this grouping of recommendations "is not tied to a specific problem statement". ● RySG and RrSG believe that Recommendation 16.3 exceeds the scope of ICANN Complaince's role, as does RrSG. ● In addition to the above-noted concerns about Recommendation 16.3, RrSG notes the following concerns: ● 16.1: "This recommendation attempts to override an existing ICANN initiative (ITI). As the ITI has been in process for a number of years, and is currently focusing on high volume and high priority items, the ITI should be allowed to continue its existing timeline as the Review Team has not provided any rationale for why RDS data should be prioritized over other action items in the ITI". ● 16.2: "The ICANN Community should not be able to dictate the composition, scope, and function of ICANN Contractual Compliance".
Dependencies:	n/a
Considerations:	Compliance has subject matter experts in the various areas listed to the extent that they are necessary for contract enforcement. For other matters and as necessary, Compliance can refer to ICANN's Chief Data Protection Officer for guidance regarding the specific areas listed. Compliance will enforce policies that have been adopted by the community and will make operational/structural changes as needed to carry out its enforcement role. RT would like Compliance to form specialized groups within Compliance to assist Law enforcement needs??? Is this related to SSAD? It is not clear what is meant by "facilitate law enforcement needs" and how that is relevant to the role of Compliance. As written, ICANN org does not have the

	authority to do this. Further, the intent of the recommendation is not clear, specifically why the existing Subject Matter Experts and Chief Data Protection Officer roles within ICANN org are inadequate to achieve the requirements of this recommendation The benefit to implementing the recommendation versus the risks and cost considerations is not clear. Elements of this recommendation require clarification regarding why the Review Team believes the existing Subject Matter Experts and Chief Data Protection Officer roles within ICANN org are inadequate to achieve the requirements of this recommendation. ICANN org will seek clarification on what is meant by "facilitate law enforcement needs" and how that is relevant to the role of Compliance.
Possible clarifying questions:	● Please clarify the purpose of the specialised groups within Compliance that understands privacy requirements and principles? ● What kind of role would these groups play? Would they focus on enforcement of privacy requirements under the RA and RAA, or the policies adopted independently by the Contracted Parties? ● Please describe any current deficiencies in enforcement of the RA/RAA privacy requirements.
Proposed recommended Board action:	Pending, likely to be rejected unless additional information shows implementation is feasible.

Recommendation 16.3	
Recommendation text:	ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3) This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.

Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	Compliance
Summary of Public Comment:	Elements of support: By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ALAC emphasizes "strong support". ● GAC suggests this grouping of recommendations "should specify clearly the need for balancing GDPR-type privacy considerations with the need to ensure access to non-personal data in line with the efforts under EPDP phase 2.A to ensure appropriate access to WHOIS registration data." Elements of concern: ● RySG is concerned that this grouping of recommendations "is not tied to a specific problem statement". ● RySG and RrSG believe that Recommendation 16.3 exceeds the scope of ICANN Complaince's role, as does RrSG. ● In addition to the above-noted concerns about Recommendation 16.3, RrSG notes the following concerns: ● 16.1: "This recommendation attempts to override an existing ICANN initiative (ITI). As the ITI has been in process for a number of years, and is currently focusing on high volume and high priority items, the ITI should be allowed to continue its existing timeline as the Review Team has not provided any rationale for why RDS data should be prioritized over other action items in the ITI". ● 16.2: "The ICANN Community should not be able to dictate the composition, scope, and function of ICANN Contractual Compliance".
Dependencies:	n/a
Considerations:	Will need to clarify the specific areas of interest from SSR2 RT, including whether it is limited to ICANN privacy policies (EPDP) or if they are asking us to audit Rrs' own policies that are not required by RAA. May be possible to conduct audits related to this as part of regular registrar audits. Possibly cannot be implemented as formulated in the ICANN system, given how the multistakeholder process works. As written, ICANN org does not have authority to audit this.

Possible clarifying questions:	Are recommended audits within this recommendation limited to ICANN privacy policies (EPDP) or to audit Rrs' own policies that are not required by RAA.?
Proposed recommended Board action:	Pending, likely to be rejected unless additional information shows implementation is feasible.

SSR2 Recommendation 17: Measuring Name Collisions

Recommendation 17.1	
Recommendation text:	ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which controlled interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the appropriate handling of sensitive data and security threats.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 17: Measuring Name Collisions (17.1 - 17.2) This recommendation can be considered implemented when ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the controlled interruption mechanism is successful. The recommendation can be considered effective when ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios. This recommendation must be completed before the next round of gTLDs.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further to it's overarching support, ALAC notes it "agrees emphatically" with this particular grouping of recommendations. ● GAC supports the request in this grouping of recommendations for a clear policy for avoiding gTLD-related name collisions to be implemented prior to further gTLD expansion. Elements of concern: ● While IPC supports this grouping of recommendations, it notes that IPC "has diverse opinions on Name Collision".

	● RySG, IPC, and Article 19 believe that this grouping of recommendations overlaps with or is in contradiction to the ongoing work related to Name Collision. For example, IPC notes “overlap with both the outputs from SubPro on Name Collision, and the Board’s recent resolution requesting the second NCAP study”. ● Article 19 encourages the recommendation to be revised “so that it is not in contradiction with the recommendations outlined under the GNSO New Subsequent Procedures Draft Final Report” and “to note that measuring name collisions should be carried out under the ongoing framework pending full completion of the work carried out by the NCAP studies group”.
Dependencies:	Dependencies on outcomes of SSAC NCAP studies.
Considerations:	It is not clear what ‘framework’ means in the context of this recommendation, or what the outcome would be. This recommendation overlaps with or has dependencies on SSAC’s Name Collision Analysis Project (NCAP) work that is currently underway.
Possible clarifying questions:	● What is meant by "a framework" in this context? ● Where are name collisions to be studied? Only at the root, or in other zones as well? ● Are any data sources beyond root server traffic to be required? In particular, did the SSR2 RT intend recursive resolver data to be necessary? ● Regarding "protected disclosure of name collision instances", under what conditions would a name collision instance be disclosed? And disclosed to whom? ● What are the criteria for determining "successful" Controlled Interruption?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 17.2	
Recommendation text:	The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 17: Measuring Name Collisions (17.1 - 17.2) This recommendation can be considered implemented when ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the controlled interruption mechanism is successful.

	The recommendation can be considered effective when ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios. This recommendation must be completed before the next round of gTLDs.
Owner (SSR2 assigned):	ICANN community and ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	Policy
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further to it's overarching support, ALAC notes it "agrees emphatically" with this particular grouping of recommendations. ● GAC supports the request in this grouping of recommendations for a clear policy for avoiding gTLD-related name collisions to be implemented prior to further gTLD expansion. Elements of concern: ● While IPC supports this grouping of recommendations, it notes that IPC "has diverse opinions on Name Collision". ● RySG, IPC, and Article 19 believe that this grouping of recommendations overlaps with or is in contradiction to the ongoing work related to Name Collision. For example, IPC notes "overlap with both the outputs from SubPro on Name Collision, and the Board's recent resolution requesting the second NCAP study". ● Article 19 encourages the recommendation to be revised "so that it is not in contradiction with the recommendations outlined under the GNSO New Subsequent Procedures Draft Final Report" and "to note that measuring name collisions should be carried out under the ongoing framework pending full completion of the work carried out by the NCAP studies group".
Dependencies:	n/a
Considerations:	Appears to be outside of ICANN org's remit to implement. The community has already agreed to the process for determining the next round of new gTLDs.

	The GNSO Council approved the SubPro PDP Final Report which includes a rec ("ICANN must have ready prior to the opening of the Application Submission Period a mechanism to evaluate the risk of name collisions in the New gTLD evaluation process as well as during the transition to delegation phase") and implementation guidance on name collisions. The GNSO also recognized that "it is up to the ICANN community and ICANN Board of Directors to determine any dependencies between the NCAP and the next round of new gTLD applications". The SubPro PDP was completed before NCAP Study 2 was approved by the Board (in March 2021). Name collision has been a topic of discussion in various parts of the community for several years. On 2 November 2017 the Board passed resolutions 2017.11.02.29 – 2017.11.02.31 requesting that the Security, Stability, and Advisory Committee (SSAC) to conduct a study to facilitate the development of policy on Collision Strings to mitigate potential harm to the stability and security of the DNS posed by delegation of such strings. The SSAC proposed a series of three studies, and an independent contractor completed Name Collision Analysis Project (NCAP) Study 1 in June 2020, which included consideration of input received through two Public Comment proceedings. Subsequently, the community-based NCAP Discussion Group redesigned the proposal for NCAP Study 2 and on 25 March 2021 the Board passed resolutions 2021.03.25.11 – 2021.03.25.14 affirming the continued relevance of the nine questions related to name collisions presented in the prior Board resolutions 2017.11.02.29 - 2017.11.02.31, especially questions concerning criteria for identifying collision strings and determining if collision strings are safe to be delegated. The Board also directed the NCAP Discussion Group to proceed with NCAP Study 2 as redesigned. The Board can request an Issue Report and require the initiation of a PDP in the GNSO, an EPDP can only be launched by a GNSO Council vote, and only in specific circumstances ("to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the ICANN Board or the implementation of such an adopted recommendation; [or] to provide new or additional policy recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists"[12].) The community has already conducted extensive policy work concerning agreed to the process for handling name collisions for the next round of new gTLDs, and NCAP is another significant community effort already underway that is expected to result in additional useful information for the Board and community on the topic.
Possible clarifying questions:	n/a

[12] GNSO Operating Rules and Procedures: Annex 4 - Expedited Policy Development Process Manual: https://gnso.icann.org/sites/default/files/file/field-file-attach/2016-12/annex-4-epdp-manual-01sep16-en.pdf

Proposed recommended Board action:	Reject because the recommendation cannot be approved in full.

SSR2 Recommendation 18: Informing Policy Debates

Recommendation 18.1	
Recommendation text:	ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 18: Informing Policy Debates (18.1 - 18.3) This recommendation can be considered implemented when ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences. This recommendation can be considered effective when the information coming from the research community on SSR-related issues is more accessible to people who are making policy decisions.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, ALAC notes that it "agrees emphatically" with this grouping of recommendations. Elements of concern: ● RySG agrees with some elements of this grouping of recommendations, but has concerns about other elements. RySG states: "In much the same way that ICANN monitors and offers neutral summary reports on legislative developments and identifier technology issues, it is reasonable for ICANN to do so for other topics related specifically to ICANN's mission and scope. However, it is unclear how recommending that ICANN offer an interpretation or analysis (including proposing additional studies) of these third-party efforts by specifically targeting only one part of the ICANN community is within either the Review Team's scope of work or ICANN's".

	• RrSG has concerns about the individual recommendations in this grouping:
	  ○ 18.1: “ICANN Org should determine which staff attends or participates in research, networking, and security conferences on behalf of ICANN Org, and how to report and/or share this information with the ICANN Community- not a Review Team. Utilizing this information to influence contracted party behaviour is outside of ICANN’s remit, and the ICANN Board should reject this recommendation”.
	  ○ 18.2: “Contract negotiations are between contracted parties and ICANN as detailed in the RAA and RA, and are not subject to public discussion and feedback from the ICANN community, including recommendations from peer-reviewed literature”.
	  ○ 18.3: “The RrSG recommends that the ICANN Board reject this recommendation, as it is not clear how the studies will be paid for, and how confirming peer-reviewed studies are beneficial or within ICANN’s remit”.

Dependencies:	n/a
Considerations:	To be treated together with 18. 2 and 18.3. based on considerations noted. • The SSR2 RT does not explain what fact-based problem recommendations 18.1 - 18.3 are trying to solve. • This recommendation implies unbounded work. There are a vast number of potential publication venues we'd have to track in a myriad of languages. As written, the rec is simply not feasible. • Further, the SSR2 RT’s intended outcome of these recommendations are not clear. Many academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money and effort would be required to sort through these papers, presentations and sessions. The determination of significance of these data would be completely subjective and would vary from community member to community member. • ICANN org currently already publishes reports of emerging technologies that are relevant to the org’s mission through its OCTO publication series, and regularly provides updates the community, for example via recent Emerging Identifier Technology sessions at ICANN58, ICANN60, ICANN64, and ICANN66. • Academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these materials. Implementing these recommendations would require additional permanent staff and the benefits of the “polling” model implied over the “push” (crowd source) model ICANN org currently uses are not clear. ICANN org suggests that public comment on this topic could be useful to understand if the community believes that additional resources should be expended on this activity.

Possible clarifying questions:	● How often does the SSR2 RT envision the report being published? For example, on a periodic basis summarizing all activity in that period, or on a per-paper, per-conference basis? ● What is the envisioned use case of these publications? ● Did the SSR2 RT consider that security meetings and conferences are frequently held under confidentiality rules that restrict the sharing of any information with those not in attendance?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 18.2	
Recommendation text:	ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 18: Informing Policy Debates (18.1 - 18.3) This recommendation can be considered implemented when ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences. This recommendation can be considered effective when the information coming from the research community on SSR-related issues is more accessible to people who are making policy decisions.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, ALAC notes that it “agrees emphatically” with this grouping of recommendations. Elements of concern:

	• RySG agrees with some elements of this grouping of recommendations, but has concerns about other elements. RySG states: "In much the same way that ICANN monitors and offers neutral summary reports on legislative developments and identifier technology issues, it is reasonable for ICANN to do so for other topics related specifically to ICANN's mission and scope. However, it is unclear how recommending that ICANN offer an interpretation or analysis (including proposing additional studies) of these third-party efforts by specifically targeting only one part of the ICANN community is within either the Review Team's scope of work or ICANN's".
	• RrSG has concerns about the individual recommendations in this grouping:
	  ○ 18.1: "ICANN Org should determine which staff attends or participates in research, networking, and security conferences on behalf of ICANN Org, and how to report and/or share this information with the ICANN Community- not a Review Team. Utilizing this information to influence contracted party behaviour is outside of ICANN's remit, and the ICANN Board should reject this recommendation".
	  ○ 18.2: "Contract negotiations are between contracted parties and ICANN as detailed in the RAA and RA, and are not subject to public discussion and feedback from the ICANN community, including recommendations from peer-reviewed literature".
	  ○ 18.3: "The RrSG recommends that the ICANN Board reject this recommendation, as it is not clear how the studies will be paid for, and how confirming peer-reviewed studies are beneficial or within ICANN's remit".

Dependencies:	Dependent on implementation of SSR2 recommendation 18.1.
Considerations:	To be treated together with 18.1 and 18.3 based on dependencies and considerations noted. The OCTO document series is mostly meant to be neutral papers (unless otherwise specified) on the technologies, and not meant to be an influencing tool for registrars and registries. This recommendation implies unbounded work. There are a vast number of potential publication venues we'd have to track in a myriad of languages. As written, the rec is simply not feasible. ICANN org currently already publishes reports of emerging technologies that are relevant to the org's mission through its OCTO publication series, and regularly provides updates the community, for example via recent Emerging Identifier Technology sessions at ICANN58, ICANN60, ICANN64, and ICANN66. Academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these materials.

	Implementing these recommendations would require additional permanent staff and the benefits of the "polling" model implied over the "push" (crowd source) model ICANN org currently uses are not clear. ICANN org suggests that public comment on this topic could be useful to understand if the community believes that additional resources should be expended on this activity.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 18.3	
Recommendation text:	ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 18: Informing Policy Debates (18.1 - 18.3) This recommendation can be considered implemented when ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences. This recommendation can be considered effective when the information coming from the research community on SSR-related issues is more accessible to people who are making policy decisions.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support:

	● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Further, ALAC notes that it "agrees emphatically" with this grouping of recommendations. Elements of concern: ● RySG agrees with some elements of this grouping of recommendations, but has concerns about other elements. RySG states: "In much the same way that ICANN monitors and offers neutral summary reports on legislative developments and identifier technology issues, it is reasonable for ICANN to do so for other topics related specifically to ICANN's mission and scope. However, it is unclear how recommending that ICANN offer an interpretation or analysis (including proposing additional studies) of these third-party efforts by specifically targeting only one part of the ICANN community is within either the Review Team's scope of work or ICANN's". ● RrSG has concerns about the individual recommendations in this grouping: ○ 18.1: "ICANN Org should determine which staff attends or participates in research, networking, and security conferences on behalf of ICANN Org, and how to report and/or share this information with the ICANN Community- not a Review Team. Utilizing this information to influence contracted party behaviour is outside of ICANN's remit, and the ICANN Board should reject this recommendation". ○ 18.2: "Contract negotiations are between contracted parties and ICANN as detailed in the RAA and RA, and are not subject to public discussion and feedback from the ICANN community, including recommendations from peer-reviewed literature". ○ 18.3: "The RrSG recommends that the ICANN Board reject this recommendation, as it is not clear how the studies will be paid for, and how confirming peer-reviewed studies are beneficial or within ICANN's remit".
Dependencies:	Dependent on implementation of SSR2 recommendation 18.1.
Considerations:	To be treated together with 18.1 and 18.2. based on dependencies and considerations noted. The OCTO document series is mostly meant to be neutral papers (unless otherwise specified) on the technologies, and not meant to be an influencing tool for registrars and registries. This recommendation implies unbounded work. There are a vast number of potential publication venues we'd have to track in a myriad of languages. As written, the rec is simply not feasible. ICANN org currently already publishes reports of emerging technologies that are relevant to the org's mission through its OCTO publication series, and regularly

	provides updates the community, for example via recent Emerging Identifier Technology sessions at ICANN58, ICANN60, ICANN64, and ICANN66. Academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these materials. Implementing these recommendations would require additional permanent staff and the benefits of the "polling" model implied over the "push" (crowd source) model ICANN org currently uses are not clear. ICANN org suggests that public comment on this topic could be useful to understand if the community believes that additional resources should be expended on this activity.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite

Recommendation 19.1	
Recommendation text:	ICANN org should complete the development of a suite for DNS resolver behavior testing.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite (19.1 - 19.2) This recommendation can be considered implemented when ICANN org finishes developing a publicly accessible test suite for community testing and research into resolver behavior. This recommendation can be considered effective when there is a test suite available with an annual update cycle that helps ensure the integrity and global availability of the DNS.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Elements of concern: ● RySG, i2Coalition, and RrSG believe this grouping of recommendations is outside of ICANN's remit, and as such do not support this grouping of recommendations. For example, RySG notes "the report fails to explain why the development of the DNS Regression Test Suite is a requirement of ICANN Org. Similar to the context for Recommendation 18, it is reasonable for ICANN to track and report on the behavior of DNS resolvers since they are a significant client of the DNS services that registries are required to support. However, the RySG considers making this an obligation or requirement of ICANN out of scope and objects to Recommendation 19".
Dependencies:	n/a

Considerations:	The testbed would operate indefinitely so as to be applicable to future changes in resolvers. This would have to be a persistent budget item in all future budget cycles for continued development and upkeep. ICANN org recommends that further clarification be sought from the implementation shepherds on what the review team intended to be done. The discussion and subsequent recommendations talk about 3 different things: - a "DNS testbed" — typically refers to verifying protocol conformance - a "regression test suite" — typically refers to a suite of tests that verify fixes to software have not been accidentally reverted (aka a "regression") - a "suite for DNS resolver behavior testing" — typically refers to the operational behavior of resolvers All of these are feasible (although by their very nature, they will never be "complete" — they'll always need to be updated every time the DNS protocol changes, bugs and subsequent fixes are introduced, and resolver behaviors change), but they have very different implications in terms of resource requirements. There are divergent views on this recommendation that the Board may wish to seek to clarify or resolve. For example, "RySG notes it is reasonable for ICANN to track and report on the behavior of DNS resolvers since they are a significant client of the DNS services that registries are required to support. However, the RySG considers making this an obligation or requirement of ICANN out of scope."
Possible clarifying questions:	● In the introductory comments, the SSR2 RT discusses a "DNS testbed", yet the recommendation title discusses a "DNS regression test suite" and the recommendations discuss a "DNS resolver behavior" test suite. These appear to be 3 different things. As such, can the implementation shepherds clarify the intent of this recommendation? ● Potential follow-up questions: ○ OCTO Text: "Which kind of resolvers specifically? Recursive only? Stub only? Both? ○ What does the team envision as the nature of the ""suite for DNS resolver testing""? A test environment with various machines and networks, or something else?
Proposed recommended Board action:	Pending, likely to be approved once further information is gathered to enable approval.

Recommendation 19.2	
Recommendation text:	ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained.

SSR2-defined measures of success:	Applies to SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite (19.1 - 19.2) This recommendation can be considered implemented when ICANN org finishes developing a publicly accessible test suite for community testing and research into resolver behavior. This recommendation can be considered effective when there is a test suite available with an annual update cycle that helps ensure the integrity and global availability of the DNS.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	OCTO
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Elements of concern: ● RySG, i2Coalition, and RrSG believe this grouping of recommendations is outside of ICANN's remit, and as such do not support this grouping of recommendations. For example, RySG notes "the report fails to explain why the development of the DNS Regression Test Suite is a requirement of ICANN Org. Similar to the context for Recommendation 18, it is reasonable for ICANN to track and report on the behavior of DNS resolvers since they are a significant client of the DNS services that registries are required to support. However, the RySG considers making this an obligation or requirement of ICANN out of scope and objects to Recommendation 19".
Dependencies:	Dependent on implementation of SSR2 recommendation 19.1.
Considerations:	The testbed would operate indefinitely so as to be applicable to future changes in resolvers. This would have to be a persistent budget item in all future budget cycles for continued development and upkeep. ICANN org recommends that further clarification be sought from the implementation shepherds on what the review team intended to be done. The discussion and subsequent recommendations talk about 3 different things: - a "DNS testbed" — typically refers to verifying protocol conformance

	- a “regression test suite” — typically refers to a suite of tests that verify fixes to software have not been accidentally reverted (aka a “regression”) - a “suite for DNS resolver behavior testing” — typically refers to the operational behavior of resolvers All of these are feasible (although by their very nature, they will never be “complete” — they’ll always need to be updated every time the DNS protocol changes, bugs and subsequent fixes are introduced, and resolver behaviors change), but they have very different implications in terms of resource requirements. There are divergent views on this recommendation that the Board may wish to seek to clarify or resolve. For example, “RySG notes it is reasonable for ICANN to track and report on the behavior of DNS resolvers since they are a significant client of the DNS services that registries are required to support. However, the RySG considers making this an obligation or requirement of ICANN out of scope.”
Possible clarifying questions:	n/a
Proposed recommended Board action:	Pending, likely to be approved once further information is gathered to enable approval.

SSR2 Recommendation 20: Formal Procedures for Key Rollovers

Recommendation 20.1	
Recommendation text:	ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for Public Comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 20: Formal Procedures for Key Rollovers (20.1 - 20.2) This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process. This recommendation can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	IANA
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● ALAC recommends further that “the experience gained from the COVID-19 pandemic be carefully considered”. Elements of concern: n/a
Dependencies:	This recommendation has dependencies on research work that has not yet been conducted, such as algorithm rolls.

Considerations:	It is not clear what outcomes the SSR2 RT is trying to achieve from the status quo apart from creating a deterministic model for its own sake. It is not clear it is going to result in better outcomes, and will likely require a lot of resources to do. Even if it was completed, it will take enduring resources to maintain it and keep it up to date. It also depends on research work that is yet to be conducted like algorithm rolls. It implies 'empirically verifiable' business process is even accomplishable, which implies we have perfect foresight into all the possible eventualities. Realistically, with a small team who conduct this work, it is far more practical and realistic to have a process that contains evaluation checkpoints that allow circumstances to be evaluated and provide for a potential course correction, rather than preemptively predict every possible outcome and make every decision point objectively determinable. ICANN org expects that this recommendation would require significant resources to implement, while the cost versus benefit is not yet clear. ICANN org notes that alternative solutions, such as a process that contains evaluation checkpoints that allow circumstances to be evaluated and provide for potential course correction, may be more appropriate. In light of these considerations, the Board may require further information, including from community engagement as appropriate, in order to take dispositive action on this recommendation.
Possible clarifying questions:	
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 20.2	
Recommendation text:	ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the root KSK rollover process.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 20: Formal Procedures for Key Rollovers (20.1 - 20.2) This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process

	after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process. This recommendation can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	IANA
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● ALAC recommends further that "the experience gained from the COVID-19 pandemic be carefully considered". Elements of concern: n/a
Dependencies:	n/a
Considerations:	Not clear what problem this recommendation is addressing. There is already a good set of community members that could carry out tabletop exercises. Cost is not insignificant. While it appears that table-top exercises would be beneficial, more information is needed to understand what the SSR2 Review Team intended to be targeted in the table-top exercises following the Root KSK rollover process.
Possible clarifying questions:	● What does the SSR2 Review Team intend to be targeted in the table-top exercises following the Root KSK rollover process?
Proposed recommended Board action:	Pending, likely to be approved once further information is gathered to enable approval.

SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators

Recommendation 21.1	
Recommendation text:	ICANN org and PTI operations should accelerate the implementation of new Root Zone Management System (RZMS) security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators (21.1) This recommendation can be considered implemented when ICANN org and PTI have a next generation RZMS that involves a robust and secure authentication and authorization model for submission and approval of the requests as well as additional functionality that would enhance the security and stability of the global DNS system. This recommendation can be considered effective when ICANN org mitigates the potential for security and stability issues that involve the misuse of the RZMS through improved identity management procedures.
Owner (SSR2 assigned):	ICANN org and PTI
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	IANA
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● RySG “is supportive of enhancing security in the Root Zone System and efforts in that direction”. Afnic offers its full support to the RySG comment. Elements of concern: n/a
Dependencies:	n/a
Considerations:	Beyond doing the development in RZMS, we need to consider: 1. The time and resources for training TLD managers 2. Develop comprehensive and secure processes around credential lifecycle management, including credential loss and staff turnover at TLD managers”

	Efforts to implement the new Root Zone Management System are already underway and ICANN org is supportive of building on existing efforts to enhance security in the Root Zone System.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

SSR2 Recommendation 22: Service Measurements

Recommendation 22.1	
Recommendation text:	For each service that ICANN org has authoritative purview over, including root zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and metrics on a single page on the icann.org website, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior).
SSR2-defined measures of success:	Applies to SSR2 Recommendation 22: Service Measurements (22.1 - 22.2) This recommendation can be considered implemented when ICANN org makes the operational status metrics on the services ICANN org supports available to the community. This recommendation can be considered effective when the community sees an increase in the transparency of ICANN org SSR-related operations.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● RySG notes strong support for this recommendation. Elements of concern: n/a
Dependencies:	n/a
Considerations:	Recommendations 22.1 and 22.2 should be considered together, as recommendation 22.2 is entirely dependent on 22.1. ICANN org agrees with the value of being more transparent with its operations.

	Changing the measurements annually may incur a significant burden on development resources, plus have an impact on the ability to compare year-on-year measurements if they are not consistently recorded. Is the scope for 22.1 limited to only IANA functions, or is it more broadly applicable to ICANN org services beyond those within the IANA functions remit? While the section suggests this is limited to IANA functions, the recommendation itself suggests it is broader, so clarity on the intended scope is needed. If the scope is strictly on IANA functions statistics, we already have a large amount of public reporting and publication of registry data on the iana.org website. Should the recommendation be interpreted to add additional pointers on the icann.org to the existing IANA datasets published elsewhere, or to duplicate the data within the ODP platform, or something else? Answers to these questions are needed before we can dig deeper into dependencies, anticipated resources/cost, and even if IANA is the right place for this recommendation to reside. Inventorying all services, establishing metrics to monitor, developing the measurement systems to collect the data, will require non-trivial effort.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 22.2	
Recommendation text:	ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 22: Service Measurements (22.1 - 22.2) This recommendation can be considered implemented when ICANN org makes the operational status metrics on the services ICANN org supports available to the community.

	This recommendation can be considered effective when the community sees an increase in the transparency of ICANN org SSR-related operations.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Low
ICANN org assessment:	
Lead:	E&IT
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. ● RySG notes strong support for this recommendation. Elements of concern: n/a
Dependencies:	Dependent on SSR2 recommendation 22.1.
Considerations:	
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

SSR2 Recommendation 23: Algorithm Rollover

Recommendation 23.1	
Recommendation text:	PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 23: Algorithm Rollover (23.1 - 23.2) This recommendation can be considered implemented when PTI updates the DPS to allow the transition from one digital signature algorithm to another and develops a consensus plan for future root DNSKEY algorithm rollovers. This recommendation can be considered effective when ICANN org is prepared for more advanced algorithms to be used for key signing, including any increases of key length and timing for key rollover.
Owner (SSR2 assigned):	PTI
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	IANA
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Elements of concern: n/a
Dependencies:	● Recommendation 23.2 (coming up with the process to do an algorithm roll) must be done before 23.1 (updating the DNSSEC Practice Statement). ● Being prepared for an algorithm roll is a part of the IANA Strategic Plan. To do this, ICANN org needs to work with the community to develop a process (rec. 23.2) and then update the DPS (rec. 23.1). Note that this does not require ICANN org to actually do the roll.

Considerations:	Implementation would require significant time and resources. This is a multi-year effort involving many parts of the technical community. Implementation would be dependent on a community effort. ● Crypto4A and Verisign provide neutral detailed comments on the technical elements of the individual recommendations in this grouping. Note that approval of these recommendations (23.1 and 23.2) does not require ICANN org to perform the roll, and that preparing for an algorithm roll is part of the PTI Strategic Plan. As such elements of work associated with Recommendation 23.1 and 23.2 are already anticipated to take place.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

Recommendation 23.2	
Recommendation text:	As a root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 23: Algorithm Rollover (23.1 - 23.2) This recommendation can be considered implemented when PTI updates the DPS to allow the transition from one digital signature algorithm to another and develops a consensus plan for future root DNSKEY algorithm rollovers. This recommendation can be considered effective when ICANN org is prepared for more advanced algorithms to be used for key signing, including any increases of key length and timing for key rollover.
Owner (SSR2 assigned):	PTI
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	IANA

Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Elements of concern: n/a
Dependencies:	Dependent on SSR2 recommendation 23.1. ● Recommendation 23.2 (coming up with the process to do an algorithm roll) must be done before 23.1 (updating the DNSSEC Practice Statement). ● Being prepared for an algorithm roll is a part of the IANA Strategic Plan. To do this, ICANN org needs to work with the community to develop a process (rec. 23.2) and then update the DPS (rec. 23.1). Note that this does not require ICANN org to actually do the roll.
Considerations:	Implementation would require significant time and resources. This is a multi-year effort involving many parts of the technical community. Implementation would be dependent on a community effort. ● Crypto4A and Verisign provide neutral detailed comments on the technical elements of the individual recommendations in this grouping Note that approval of these recommendations (23.1 and 23.2) does not require ICANN org to perform the roll, and that preparing for an algorithm roll is part of the PTI Strategic Plan. As such elements of work associated with Recommendation 23.1 and 23.2 are already anticipated to take place.
Possible clarifying questions:	n/a
Proposed recommended Board action:	Approve.

SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process

Recommendation 24.1	
Recommendation text:	ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process (24.1 - 24.2) This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome. This recommendation can be considered effective when ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	GDS
Summary of Public Comment:	Elements of support: ● By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Elements of concern: n/a
Dependencies:	n/a
Considerations:	In order for the Board to take dispositive action, the Board may wish to consult with the Implementation Shepherds on this recommendation. ICANN org notes that while it has conducted EBERO testing on “live” gTLDs, these were gTLDs that were in the process of being terminated. If the SSR2 Review Team is recommending that ICANN org conduct EBERO testing on “live” gTLDs with registrations, this would be an extremely complex process.

	Based on this, ICANN org recommends that the following clarifying questions be sent to the Implementation Shepherds: ● Can the SSR2 Implementation Shepherds provide further detail as to whether the recommendation intends for testing of the full EBERO process to be conducted on a live gTLD? Similarly, can the SSR2 Implementation Shepherds provide further details regarding expectations for "coordinat[ing] with the ICANN contracted parties", as the EBERO process is foreseen to occur when a contracted party is unable or unwilling to assist in an emergency transfer?
Possible clarifying questions:	What involvement did the SSR2 RT envision the contracted parties would have in the testing process, given that the EBERO process is designed assuming that a Registry Operator is unable to or unwilling to assist in an emergency transfer?
Proposed recommended Board action:	Pending, hold to seek clarity or further information.

Recommendation 24.2	
Recommendation text:	ICANN org should make the Common Transition Process Manual easier to find by providing links on the EBERO website.
SSR2-defined measures of success:	Applies to SSR2 Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process (24.1 - 24.2) This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome. This recommendation can be considered effective when ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.
Owner (SSR2 assigned):	ICANN org
Priority (SSR2 assigned):	Medium
ICANN org assessment:	
Lead:	GDS
Summary of Public Comment:	Elements of support:

	• By way of their overarching support for all recommendations in the SSR2 Final Report, INTA, BC, IPC, and ALAC support this grouping of recommendations. Elements of concern: n/a
Dependencies:	None
Considerations:	The SSR2 Review Team noted that the "EBERO processes are documented in the Common Transition Process Manual, that document was extremely difficult to find as it is embedded in the EBERO Agreement. ICANN org is able to update the EBERO website with links to the Common Transition Process Manual, subject to prioritization, costing and implementation considerations. It may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ICANN org's Information Transparency Initiative (ITI).
Possible clarifying questions:	None
Proposed recommended Board action:	Approve.

DRAFT Scorecard: Final SSR2 Review Team Recommendations - Board Action 22 July 2021
See Related Board Resolution and Rationale for more details

SSR2 recommendation	SSR2-defined measures of success	Board action
Recommendations the Board approves, subject to prioritization, risk assessment and mitigation, costing and implementation considerations; and recommendations that the Board approves, with the understanding that they are already fully implemented		
1.1: The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations) **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN Board and ICANN org	n/a	The Board approves Recommendation 1.1, subject to prioritization, risk assessment and mitigation, costing and implementation considerations. Under the Bylaws, the SSR2 Review Team is empowered to determine the extent to which ICANN org has completed implementation of the SSR1 recommendations and has done so as part of its final report. To the extent this recommendation is intended to establish a collaborative mechanism to progress implementation of SSR2 recommendations with input from the SSR2 Implementation Shepherds, the Board approves this recommendation. The Board notes, however, that as a formal matter the Bylaws (Section 4.6(b)(iii)) reserve to SSR3 (or other future SSRs) the role of final assessment of the completion of recommendations from prior SSRs, including those that the SSR2 Review Team assessed. The Board directs ICANN's President and CEO, or his designee(s), to undertake a thorough analysis of the SSR2 Review Team's finding pertaining to the implementation of SSR1 recommendations and complete ICANN org's implementation, where appropriate, subject to prioritization, availability of resources, cost-effectiveness, and relevancy of the recommendations given the ever-changing landscape of the security, stability, and resiliency of the Internet's unique identifiers.
4.1: ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3):** This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.	The Board approves Recommendation 4.1, with the understanding that this recommendation is already fully implemented, and no further action is required. The Board understands that ICANN org already has policies, plans and programs in place through which Recommendation 4.1 has already been implemented, and the Board continues its oversight role over ICANN org's risk management efforts. The Board is supportive of ICANN org in continuing the risk management activities that it is already carrying out.
5.1: ICANN org should implement an ISMS and be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The	**SSR2-defined measures of success for Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1**	The Board accepts ICANN org's representation that, once migration to the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework is fully

plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**- 5.4):** This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.	complete, Recommendations 5.1 and 5.2 will be implemented. Therefore, the Board approves recommendations 5.1 and 5.2, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations, noting that substantial parts of the recommendation are already being addressed or will be addressed once ICANN org's migration to the NIST Cybersecurity Framework is fully complete.
5.2: Based on the ISMS, ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
9.1: The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse related obligations in contracts, baseline agreements, temporary specifications, and community policies. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN Board	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4):** This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).	The Board accepts ICANN org's representation that the Contractual Compliance operations that ICANN org has in place already meet the SSR2 Review Team's defined measures of success for Recommendation 9.1. Therefore, the Board approves this recommendation, with the understanding that this recommendation is already fully implemented and no further action is required.
10.1: ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct—ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-	**SSR2-defined measures of success for Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (10.1 - 10.3):** This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date. This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy	To the extent that this recommendation is intended to enhance transparency, accountability, and clarity of ICANN org's work on Domain Name System (DNS) security threat mitigation through its existing contractual and compliance mechanisms, and thereby facilitate ongoing community discussions around definitions of DNS security threats, the Board approves this recommendation subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board notes that these considerations may be particularly important as definitions, procedures and protocols may evolve over time. In this regard, the Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of

related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.	ICANN org's Information Transparency Initiative (ITI).
16.1: ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the RDS. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3):** This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.	The Board approves Recommendation 16.1, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ITI.
21.1: ICANN org and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org and PTI	**SSR2-defined measures of success for Recommendation 21: Improve the Security of Communications with TLD Operators (21.1):** This recommendation can be considered implemented when ICANN org and PTI have a next-generation RZMS that involves a robust and secure authentication and authorization model for submission and approval of the requests as well as additional functionality that would enhance the security and stability of the global DNS system. This recommendation can be considered effective when ICANN org mitigates the potential for security and stability issues that involve the misuse of the RZMS through improved identity management procedures.	The Board notes that efforts to implement the new Root Zone Management System are already underway and the Board is supportive of building on existing efforts to enhance security in the Root Zone System. The Board notes that Recommendation 23.2 must be completed before the DNSSEC Practice Statement can be updated as called for in Recommendation 23.1. Further, the Board notes that preparing for an algorithm roll is part of the Public Technical Identifiers (PTI) Strategic Plan. As such, some elements of work associated with these recommendations are already anticipated to take place. The Board approves Recommendations 21.1, 22.1, 22.2, 23.1 and 23.2, subject to prioritization, risk assessment and mitigation, costing and other implementation considerations.
22.1: For each service that ICANN org has authoritative purview over, including root-zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and	**SSR2-defined measures of success for Recommendation 22: Service Measurements (22.1 - 22.2):** This recommendation can be considered implemented when ICANN org makes the operational status metrics on the services ICANN org supports available to the community. This	

metrics on a single page on the icann.org web site, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior). **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org	recommendation can be considered effective when the community sees an increase in the transparency of ICANN org SSR-related operations.	
22.2: ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org		
23.1: PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS. **SSR2 designated priority:** Medium **SSR2 designated owner:** PTI	**SSR2-defined measures of success for Recommendation 23: Algorithm Rollover (23.1 - 23.2):** This recommendation can be considered implemented when PTI updates the DPS to allow the transition from one digital signature algorithm to another and develops a consensus plan for future root DNSKEY algorithm rollovers. This recommendation can be considered effective when ICANN org is prepared for more advanced algorithms to be used for key signing, including any increases of key length and timing for key rollover.	
23.2: As a root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018. **SSR2 designated priority:** Medium **SSR2 designated owner:** PTI		
24.2: ICANN org should make the Common Transition Process Manual	**SSR2-defined measures of success for Recommendation 24: Improve Transparency and**	The Board approves recommendation 24.2, subject to prioritization, risk assessment and mitigation, costing and

easier to find by providing links on the EBERO website. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**End-to-end Testing for the EBERO Process (24.1 - 24.2):** This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome. This recommendation can be considered effective when ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.	other implementation considerations. The Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ITI.
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations the Board rejects because the recommendation cannot be approved in full		
4.2: ICANN org should adopt and implement ISO 31000 "Risk Management" and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures). **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3):** This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.	The Board notes that ICANN org has a strong, clearly documented risk management program, but not as envisioned by SSR2, as written. Thus, the Board agrees with the recommendation in principle, and considers the intent of the recommendation achieved through ICANN org's current operations. However, the Board cannot approve the portion of the recommendation that specifies that ICANN org "adopt and implement International Standardization Organization (ISO) 31000 'Risk Management' and validate its implementation with appropriate independent audits…" because it is not clear what risks would be mitigated , nor what benefit would be derived in expanding significant resources to switch from the current risk-management process. The Board supports ICANN org's risk management operations already in place. In light of the above considerations, and the fact that approval of the recommendation would require ICANN org to adopt and implement ISO 31000, while the Board agrees in principle with the intent of the recommendation, the Board rejects recommendation 4.2. The Board encourages ICANN org to continue following industry best practices and look for ways to strengthen its risk management practices as it evolves its operations as part of its continuous improvement.
8.1: ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the	**SSR2-defined measures of success for Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties (8.1):** This recommendation can be considered implemented when ICANN org has included abuse and security specialists in these negotiations and the management of the domain name system aligns with public safety	The Board notes that the aspect of the recommendation that calls for the introduction of a third party into the bilateral negotiation process is not proper or feasible. The Registry Agreement and Registrar Accreditation Agreement do not allow for third-party beneficiaries. The Board notes that ICANN org negotiates in the broader interest of ICANN, including the public interest, and does not represent the interests of the domain industry. The Board also understands that parts of the ICANN community have concerns, as

domain name system for end-users, businesses, and governments. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	and consumer interests, and not just those of the domain name industry. This recommendation can be considered effective when a broader and more balanced set of stakeholders are able to have direct input into the contracts negotiated with contracted parties.	reflected through the public comments, about how Contracted Party agreements are negotiated, and acknowledges that it is important to listen carefully to the community as negotiations proceed and decisions are made. ICANN org also has an important enforcement role once items are incorporated into contracts. The Board further notes that recommendation 8.1 is not allowed under the provisions of the RA and RAA. While the agreements do provide for a "Working Group", these have contractually specific meanings that are not aligned with this recommendation. For example, in the case of the RA, a "Working Group" is defined as: "representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements (excluding bilateral amendments pursuant to Section 7.6(i)) Neither the Board or ICANN org is involved in the appointment of these contractual "Working Groups". Further, the Board and ICANN org cannot bring about contractual changes unilaterally. In light of the above considerations, the Board rejects this recommendation. The Board encourages ICANN org to continue bilateral discussions with the contracted parties in a way that enhances the security, stability, and resiliency of the DNS and to strive to have these bilateral discussions be transparent to the general public, in order to continue building trust.
9.4: ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4):** This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community. This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence based Security Improvements).	The Board accepts in principle the idea of improving the tools that the ICANN org Contractual Compliance team has available to it in order to enforce policies that have been adopted by the community. However, the Board cannot approve the part of the recommendation that contemplates "measures that would require changes to the contracts" as such changes cannot be undertaken by either the Board or ICANN org unilaterally. As such, the Board rejects this recommendation given that it is not consistent with the role and authority of ICANN org's Contractual Compliance team. The Board encourages ICANN org's Contractual Compliance team to continue pursuing new tools that will help improve its work.

10.2: Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (10.1 - 10.3):** This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date. This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.	The Board rejects Recommendation 10.2, as neither ICANN org nor Board can unilaterally establish a cross-community working group. However, the Board notes that the community continues its discussions over DNS security threat mitigation. Discussions include questions around the definitions and scope of DNS security threats that can be considered as coming within ICANN's remit and the extent to which policy or other community work may be required to supplement efforts already underway, such as industry-led initiatives. The Board is fully supportive of this effort and remains committed to this important work through facilitation and the convening of diverse relevant groups with diverse viewpoints. The Board rejects Recommendation 10.3 due to its dependencies on Recommendation 10.2; however, the Board supports using consensus definitions consistently.
10.3: Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page. **SSR2 designated priority:** High SSR2 designated owner: **ICANN org**		
17.2: The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN community and ICANN org.	**SSR2-defined measures of success for Recommendation 17: Measuring Name Collisions (17.1 - 17.2):** This recommendation can be considered implemented when ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the controlled interruption mechanism is successful. The recommendation can be considered effective when ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios. This recommendation must be completed before the next round of gTLDs.	The Board rejects Recommendation 17.2, as the Board does not have the authority to develop policy. The Board notes that the community has already conducted extensive policy work concerning the process for handling name collisions for the next round of New Generic Top-Level Domains (new gTLDs), and the Security and Stability Advisory Committee (SSAC) Name Collision Analysis Project (NCAP) is another significant community effort already underway that is expected to result in additional useful information for the Board and community on the topic. Given the ongoing work in this area, including the NCAP studies, the Board understands that the results of those studies may have implications for SSR in the context of a future round of new gTLDs.
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations the Board rejects		
2.1: ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security	**SSR2-defined measures of success for Recommendation 2: Create a C-Suite Position**	The Board notes that it has an oversight role; it is the responsibility of the ICANN President and CEO to structure ICANN

Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	**Responsible for Both Strategic and Tactical Security and Risk Management (2.1 - 2.4):** This recommendation can be considered implemented when ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations. This recommendation can be considered effective when ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.	org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability. The Board supports ICANN org's decision to distribute the various security functions to the relevant functional areas within the organization because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages). These functional teams work closely not only with one another but also with the Board Risk Committee, which provides oversight as to the risk based functions for which ICANN org is responsible. In addition ICANN org's Risk Management function is currently already assumed by a C-suite position, and org has put in place a CEO Risk Management Committee to oversee all risk management activities of the org, including the CEO and all C-Suite executives in charge of any security matters, whether DNS-related, cyber- and system- related and physical related. The CEO Risk Management Committee is therefore a mechanism that provides ICANN org with the overarching perspective and ability to centrally act on all security matters. It is not clear what issues the SSR2 Review Team intends the proposed C-Suite role and reorganization would address, or why the SSR2 Review Team believes that the creation of the C-Suite role and reorganizing structures that ICANN org intentionally distributed for efficiency and focus would have sufficient impact on those issues to justify the risk and disruption to staff and cost. In light of the above considerations, the Board rejects Recommendations 2.1, 2.2, 2.3 and 2.4. However, the Board agrees with increased reporting and periodic communication of SSR activities. This is already partially performed as part of the current annual planning process but could be enhanced consistently with the presumed intent of the Recommendation 2.2
2.2: ICANN org should include as part of this role's description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
2.3: ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
2.4: ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and		

responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, supply chains for hardware and software, and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
14.1: ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2):** SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.	The Board notes that Temporary Policies can only be established by the Board upon specific requirements, such as when the Board "reasonably determines that such modifications or amendments are 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, the DNS or the Internet." The Board notes that Recommendation 14.1 does not provide such emergency grounds, and as such rejects this recommendation and the recommendations dependent on its implementation (14.3, 14.4, 14.5, 15.1 and 15.2). Further, the Board notes that, while it can request an Issue Report and Policy Development Process (PDP) be done by the Generic Names Supporting Organization (GNSO), an Expedited Policy Development Process (EPDP) can only be launched by a GNSO Council vote, and only in specific circumstances. The Board notes that Recommendation 15.1 does not meet these requirements. The Board, consistent with its action on the Competition, Consumer Trust, and Consumer Choice (CCT) Review Team recommendations, will not take the place of the community within the multistakeholder model and initiate a PDP upon a Specific Review team's recommendation. As such, even without dependency on Recommendation 14.1, the Board would not be in a position to approve Recommendations 15.1 and 15.2.
14.3: Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and then issue a notice to the relevant party. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
14.4: ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Compliance should move to the de-accreditation process. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
14.5: ICANN org should consider offering financial incentives:		

contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
15.1: After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported EPDP to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
15.2: The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org		
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations the Board determines to be pending, likely to be approved once further information is gathered to enable approval		

5.4: ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes to manage risk, security, and vulnerabilities. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4):** This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.	While implementation of the recommendation appears feasible, the Board requires clarification on several elements of this recommendation in order to accurately assess resource requirements and enable approval. For example, the required granularity of the reports expected by the SSR2 Review Team, and what entities the SSR2 Review Team envisioned ICANN org report out to "beyond" the ICANN community are not clear. The Board directs the ICANN President and CEO, or his designee(s) to seek clarifications from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendation 5.4 can be approved.
19.1: ICANN org should complete the development of a suite for DNS resolver behavior testing. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org **19.2:** ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 19: Complete Development of the DNS Regression Test Suite (19.1 - 19.2):** This recommendation can be considered implemented when ICANN org finishes developing a publicly accessible test suite for community testing and research into resolver behavior. This recommendation can be considered effective when there is a test suite available with an annual update cycle that helps ensure the integrity and global availability of the DNS.	The Board notes that the SSR2 Review Team's discussion and recommendations in the Final Report refer to three different things: a "DNS testbed"; a "regression test suite"; and "a suite for DNS resolver behaviour testing." While any of these may be feasible, the Board requires clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent in order to accurately assess resource requirements. The Board directs the ICANN President and CEO, or his designee(s), to seek clarifications from the SSR2 Implementation Shepherds on elements of these recommendations that are not clear. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendations 19.1 and 19.2 can be approved. Further, the Board understands that the testbed would operate indefinitely so as to be applicable to future changes in resolvers. If the Board eventually approves this recommendation, maintenance of a testbed environment would have to be a persistent budget item in all future budget cycles for continued development and upkeep.
20.2: ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root KSK rollover process. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 20: Formal Procedures for Key Rollovers (20.1 - 20.2):** This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process. This recommendation	While the recommendation appears feasible and the Board believes that table-top exercises would be beneficial, more information is needed to understand what the SSR2 Review Team intended to be targeted in the table-top exercises following the Root key signing key (KSK) rollover process. The Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will

	can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable. This recommendation must be completed in conjunction with each key rollover.	inform the Board's decision on next steps and whether Recommendation 20.2 can be approved.
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations that the Board determines to be pending, holding to seek clarity or further information		
3.1: The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation SSR2-defined measures of success for Recommendation 3: Improve SSR-related Budget Transparency (3.1 - 3.3):** This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget.	The Board notes that, as written, successful implementation of Recommendations 3.1 - 3.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. The Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent, and if implementation of these recommendations can be considered effective after the Board rejects Recommendation 2, thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendations 3.1, 3.2, and 3.3 to that new office. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
3.2: The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN Strategic Plan goals and objectives. ICANN org should implement those mechanisms through a consistent, detailed, annual budgeting and reporting process. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN Board and ICANN org		
3.3: The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN Board and ICANN org		
4.3: ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-	**SSR2-defined measures of success for Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3):** This recommendation can be considered implemented when	The Board notes that as written, successful implementation of Recommendation 4.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a CSO or CISO at

Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications). **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.	the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. In light of this dependency on Recommendation 2, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective after the Board rejects Recommendation 2 thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendation 4.3. The Board has a concern with accepting a recommendation for which implementation can never be deemed successful or effective. Further, the Board notes it is the responsibility of the ICANN President and CEO, or his designee(s), to structure ICANN org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability. In addition, it is not clear as to what the SSR2 Review Team envisioned would be mitigated, nor what cost/benefit would be derived from the recommended structure. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
5.3: ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4):** This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.	The Board understands that ICANN org's Engineering & Information Technology (E&IT) function already requires all vendors and service providers to have a risk assessment performed and documented which meets industry-standard requirements. In order to accurately assess resource requirements and feasibility, the Board requires clarification from the SSR2 Implementation Shepherds as to if the SSR2 Review Team's intent was to expand this risk assessment to all ICANN org vendors and service providers. The Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherd as to the SSR2 Review Team's intended scope of this recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
7.1: ICANN org should establish a Business Continuity Plan for all the	**SSR2-defined measures of success for Recommendation**	The Board notes that the SSR2 Review Team states successful measures of

systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	**7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5):** This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.	implementation for these recommendations as: "This recommendation can be considered implemented when ICANN org's Business Continuity (BC) and Disaster Recovery (DR) plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational." The Board is placing Recommendation 7.4, which calls for the "non-U.S., non-North American site" into "pending, likely to be rejected unless additional information shows implementation is feasible." As such, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of these recommendations can be considered effective in the event that the Board rejects Recommendation 7.4 regarding opening a non-U.S., non-North American site, and that portion of the success measure cannot be achieved. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
7.2: ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO). **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
7.3: ICANN org should also establish a DR Plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
7.5: ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
9.3: ICANN org should have compliance activities audited externally at least annually and	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce**	The Board notes that some elements of this recommendation are not clear, such as what would be audited, against what

publish the audit reports and ICANN org response to audit recommendations, including implementation plans. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**Compliance (9.1 - 9.4):** This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community.	criteria, by whom, or why an external auditor would be required. The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the SSR2 Implementation Shepherds on elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
11.1: The ICANN community and ICANN org should take steps to ensure that access to CZDS data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN community and ICANN org	**SSR2-defined measures of success for Recommendation 11: Resolve CZDS Data Access Problems (11.1):** This recommendation can be considered implemented when ICANN org and the community makes access to CZDS data available in a timely manner and without unnecessary hurdles to requesters. This recommendation can be considered effective when ICANN org reports a decrease in the number of zone file access complaints and improves the ability for researchers to study the security-related operations of the DNS.	The Board notes that some elements of this recommendation are not clear. For example, the Board notes that ICANN org is currently in the process of implementing recommendations from SAC097, which calls for ICANN org to revise "the [Centralized Zone Data Service] CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default." It is not clear what additional work is needed to sufficiently implement the SSR2 Review Team's Recommendation 11.1 or how the existing work already being performed on CZDS access is insufficient. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
12.1: ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review (12.1 - 12.4):** This recommendation can be considered implemented when ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data. This recommendation can be considered effective when all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.	The Board acknowledges the extensive community and ICANN org efforts currently going on around DNS security threats. The Board directs the ICANN President and CEO, or his designee(s), to evaluate how this grouping of recommendations, along with other recommendations that pertain to DNS security threats should be considered in a coordinated way, including through ICANN org's program dedicated to DNS security threats mitigation. This information will inform the Board's decision on next steps. The Board notes, however, that beyond the interdependencies related to the extensive community and ICANN org efforts around DNS security threats, there may be additional challenges associated with implementation of some of these recommendations that the Board would require to be addressed before determining if these recommendations can be approved.
12.2: ICANN org should structure its agreements with data providers to allow further sharing of the data for non-commercial use, specifically for validation or peer-reviewed scientific research. This special no-fee non-commercial license to use the data may involve a time-delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN web site. ICANN org should terminate any contracts that do not		

allow independent verification of methodology behind blocklisting. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		
12.3: ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		
12.4: ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		
13.1: ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all gTLDs; the participation of each ccTLD would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting (13.1 - 13.2):** This recommendation can be considered implemented when ICANN org simplifies the process of submitting and receiving abuse complaints and offers insight into the number of complaints and some metadata (e.g., type of abuse reported, dates, time to resolution) for researchers and community members. This recommendation can be considered complete when the portal is up and running. This recommendation can be considered effective when contracted parties have to spend less time on misdirected complaints, and the research community as well as the broader ICANN community can see and study the associated data about those complaints.	
13.2: ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS.		

SSR2 designated priority: High **SSR2 designated owner:** ICANN org		
14.2: To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (14.1 - 14.5); and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (15.1 - 15.2):** SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements. SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties. The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do. These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time. ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.	The Board directs the ICANN President and CEO, or his designee(s) to regard the measures of success as defined by the SSR2 Review Team for Recommendations 14 and 15, and evaluate how this recommendation, along with other recommendations that pertain to DNS security threats, should be considered in a coordinated way, including through the ICANN org program dedicated to DNS security threats mitigation and ongoing projects such as the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project, and Domain Abuse Activity Reporting System (DAAR). . This information will inform the Board's decision on next steps.
17.1: ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which Controlled Interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the	**SSR2-defined measures of success for Recommendation 17: Measuring Name Collisions (17.1 - 17.2):** This recommendation can be considered implemented when ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the controlled interruption	The Board notes that Recommendation 17.1 has dependencies on the SSAC NCAP. The output of the NCAP studies will inform the Board's decision on next steps. The Board noted such overlap in its comments on the SSR2 Review Team draft report, and encouraged the SSR2 Review Team to consider how its recommendations may be consolidated into or passed through to ongoing work.

appropriate handling of sensitive data and security threats. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	mechanism is successful. The recommendation can be considered effective when ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios.	
18.1: ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 18: Informing Policy Debates (18.1 - 18.3):** This recommendation can be considered implemented when ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences. This recommendation can be considered effective when the information coming from the research community on SSR-related issues is more accessible to people who are making policy decisions.	While the Board agrees that there is merit to ICANN org performing an evaluation to ensure that it is tracking at an appropriate level to the work that ICANN does, the Board notes that many academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these materials. In this manner, Recommendations 18.1 - 18.3 imply unbounded work. The Board would like to better understand the community's views as to if ICANN org should expend additional resources on this activity, in light of current existing work. The Board directs the ICANN President and CEO, or his designee(s), to perform an evaluation of its tracking efforts already underway and provide this to the Board to ensure that ICANN org is tracking at an appropriate level to the work that ICANN does. Further, the Board directs the ICANN President and CEO, or his designee(s) to engage the community to understand if ICANN org should expend additional resources on this activity, in light of current existing work. This information will inform the Board's decision on next steps.
18.2: ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org		
18.3: ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org		
20.1: ICANN org should establish a formal procedure, supported by a	**SSR2-defined measures of success for Recommendation**	The Board expects that this recommendation would require significant

formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for public comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**20: Formal Procedures for Key Rollovers (20.1 - 20.2):** This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process. This recommendation can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable.	resources to implement, while the cost versus benefit is not clear. Further, the Board notes that this recommendation has dependencies on research work that has not yet been conducted, such as algorithm rolls. The Board notes that alternative solutions, such as a process that contains evaluation checkpoints that allow circumstances to be evaluated and provide for potential course correction, may be more appropriate. In light of these considerations, the Board requires further information, including from community engagement as appropriate, in order to take dispositive action on this recommendation. The Board directs the ICANN President and CEO, or his designee(s) to gather further information, including via community engagement and engagement with the SSR2 Implementation Shepherds as appropriate on this recommendation. This information will inform the Board's decision on next steps.
24.1: ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised, and publish the results. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process (24.1 - 24.2):** This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome. This recommendation can be considered effective when ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.	The Board notes that some elements of this recommendation are not clear. For example, it is not clear if the SSR2 Review Team's intent is for ICANN org conduct Emergency Back-end Registry Operator (EBERO) testing on "live" gTLDs with registrations. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
SSR2 recommendation	**SSR2-defined measures of success**	**Board action**
Recommendations the Board determines to be pending, likely to be rejected unless additional information shows implementation is feasible		
6.1: ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs**.** **SSR2 designated priority:** High	**SSR2-defined measures of success for Recommendation 6: SSR Vulnerability Disclosure and Transparency (6.1 - 6.2):** This recommendation can be considered implemented when ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting. These recommendations can be considered effective when ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.	The Board notes that several elements of the recommendation are not clear. For example, as written, it is not clear how ICANN org should implement the recommendation in the event that there is not voluntary adoption, and may require a GNSO Policy Development Process. Possibly, the SSR2 Review Team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and Memorandums of Understanding (MOUs)". If this is the intent, while the Board supports contracted parties using best practices that align with the goals and objectives outlined in ICANN's Strategic Plan, making implementation of best practices mandatory would be a policy

SSR2 designated owner: ICANN org		matter and not something ICANN org or Board can unilaterally impose in "contracts, agreements, and MOUs." Other elements of this recommendation that require clarification include, for example, how should SSR best practices/objectives be identified? How should ICANN org measure adoption? What is the threshold to evaluate ICANN org's promotional efforts as insufficient? The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
6.2: ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.		The Board notes there are three components of this recommendation, which each have different considerations. While ICANN org already does some of the things called for within the recommendation as ICANN org noted in its comments on the SSR2 Review Team draft report, the recommendation's focus on disclosure appears difficult or nearly impossible to implement. The Board directs the ICANN President and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation and the possible process to implement it with the relevant parties. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
7.4: ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5):** This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.	The Board does not have enough information to consider resource implications of implementing this recommendation versus the expected benefit. The Board notes that in its comment on the SSR2 Review Team draft report, ICANN org asked the SSR2 Review Team to provide clear justification as to why it believes the benefits of a third disaster recovery site justifies the costs of such a site. While the recommendation states that the new site could replace "either the Los Angeles or Culpeper sites", the requested cost/benefit information is not provided in the SSR2 Review Team Final Report. Further, the Board notes Section 4.2 of the Internet Assigned Numbers Authority (IANA) Naming Function Contract that prohibits IANA operations outside of the United States, and as such, the Board understands that implementation of this recommendation as written is not currently feasible for some portions of the IANA functions. These restrictions could be removed through contract amendments if there were a desire to do so from the ICANN community, which would require community consultation and discussion. The Board directs the ICANN President

		and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand elements of this recommendation that are not feasible as written, or are not clear, including if the SSR2 Review Team considered the benefit versus cost considerations. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps, which may include wider community consultation.
9.2: ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4)**: This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community.	The Board notes that ICANN org does not have authority to require validation beyond what is in the Registry Agreement and Registrar Accreditation Agreement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, including the authority the SSR2 Review Team understood that ICANN org's Contractual Compliance team has to carry out the recommended actions. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
16.2: ICANN org should create specialized groups within the contract compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems). **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SR2-defined measures of success for Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3):** This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.	The Board is not clear as to what is meant by "facilitate law enforcement needs" and how that is relevant to the role of ICANN org's Contractual Compliance team. As written, ICANN org does not have the authority to do this. Further, the intent of the recommendation is not clear, specifically why the SSR2 Review Team understands the existing subject matter experts and Chief Data Protection Officer roles within ICANN org are inadequate to achieve the requirements of this recommendation. The Board understands that ICANN org's Contractual Compliance team has subject matter experts in the areas listed to the extent that they are necessary for contract enforcement. For other matters and as necessary, ICANN org's Contractual Compliance members can refer to ICANN org's Chief Data Protection Officer for guidance regarding the specific areas listed. Through the Contractual Compliance team, ICANN org enforces policies that have been adopted by the community and makes operational and structural changes as needed to carry out its enforcement role. The Board directs the ICANN President and CEO, or his designee(s), to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, as well as other

		elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
16.3: ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org		The Board noted in its comment on the SSR2 Review Team draft report, ICANN org does not specifically require registrars to have "privacy policies." ICANN org's Contractual Compliance team cannot audit something that is not an ICANN contractual requirement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.