SAC 043
SSAC Comment on the JAS Report on the IANA Process for Implementing Root Zone Change Requests and on the IANA Explanatory Memoranda

A Comment from the ICANN
Security and Stability
Advisory Committee
(SSAC)
05 October 2010

Preface

This is a Comment by the Security and Stability Advisory Committee (SSAC) on the following report by JAS Communications LLC: "IANA Process for Implementing Root Zone Change Requests: Review and Assessment of Risk Management Strategy and Comparison of Implementation Options" posted on 19 April 2010. This also is a comment on the IANA response to the JAS report recommendations, the "Explanatory Memoranda Regarding the Report 'IANA Process for Implementing Root Zone Change Requests – Review and Assessment of Risk Management Strategy and Comparison of Implementation Options.'"

The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this Comment, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this Comment, are at end of this Comment.

Table of Contents

1. Introduction

In August 2009, the Internet Corporation for Assigned Names and Numbers (ICANN) engaged JAS communications LLC (JAS) to provide a risk assessment of the ICANN Internet Assigned Numbers Authority (IANA) root zone change process. The focus was to analyze the current manual processes and procedures and the proposed automated processes and procedures. JAS conducted the assessment from August through November 2009 and submitted its results to ICANN with nine recommendations for improved security and stability of operations. These recommendations reflected the perspective of JAS on ICANN's root zone change processes and procedures, and were intended to focus solely on the roles and responsibilities on ICANN as the IANA functions operator. The resulting report, "IANA Process for Implementing Root Zone Change Requests: Review and Assessment of Risk Management Strategy and Comparison of Implementation Options," was posted on 19 April 2010.[1]

Members of the SSAC formed a Work Party to discuss this report and to consider whether to draft formal comments. The Work Party also reviewed the IANA response to the JAS recommendations: "Explanatory Memoranda Regarding the Report 'IANA Process for Implementing Root Zone Change Requests – Review and Assessment of Risk Management Strategy and Comparison of Implementation Options.'"[2] The Work Party subsequently drafted the following comments to both the JAS report and the IANA response, which it provided to the full SSAC to review and consider. The SSAC welcomes the opportunity to comment on the JAS report and the IANA response. This Comment is organized as follows:

1. Introduction: An explanation of the genesis of this Comment;
2. General comments on the report;
3. Comments on the methodology and modeling;
4. Comments on the report's recommendations;
5. Comments on specific points;
6. Comments on the IANA Explanatory Memoranda; and
7. Acknowledgements, statements of interest, objections and withdrawals.

1 See: <http://www.icann.org/en/reviews/iana/iana-root-zone-process-review-16jun10-en.pdf>.

2 See <www.icann.org/en/reviews/iana/iana-root-zone-process-review-16jun10-en.pdf>.

2. General Comments on the Report

The JAS report is focused on security, stability, and resiliency. While there are some good points in the JAS report, problems with the JAS report's model and analysis lead the SSAC to question its validity and utility. In particular, the SSAC makes the following three general comments on the report:

1. The JAS report raised the issue of lack of better documentation on how a root zone change works, particularly in the presence of the root zone management system. The SSAC agrees with this point. In particular, the report noted that non-disclosure agreements related to some steps prevents them from being fully documented. A risk analysis may be considered appropriate to define the number of people, which shall be under a non-disclosure agreement to restore functionality if an error occurs.
2. The JAS report analyzes the difficulty of carrying out the IANA function if there is a significant, extended outage of the Internet, and, on the basis of the dependency on email, suggests the IANA function should be provisioned with backup communications systems. The SSAC finds this to be a compound error in the JAS report and the threat model is not correct. First, there is no credible basis for assuming the Internet will suffer a significant extended outage. The document cited is a Business Roundtable report, which the SSAC did not accept as credible. Second, if the Internet were down for an extended period of time, unless the IANA function were relevant to bringing it back up, the SSAC doubts that anyone would care whether the IANA function was operating. Finally, the SSAC disagrees with the JAS report regarding the need for IANA to have a backup communication system to be used if the Internet is down an extended period of time, and wonders whether the JAS considered the existence of other actors acting promptly if such event happened.
3. Finally, the SSAC notes that the way JAS conducted its report, by bringing together several comments with analysis and recommendations, suggests that it was completed in a transparent and independent manner. However, the SSAC thinks that the report should be followed by analysis and comments by ICANN. In particular, such reports should be followed by a determination by ICANN as to which recommendations were implemented and the affect of those recommendations on the IANA operations.

3. Comments on the Methodology and Modeling

The SSAC thinks that the assessment in the JAS report has several limitations in its methodology as follows:

1. The JAS has made a model of the root zone change process itself. However, this model only looks at risks of failures and error rates for sub-systems, rather than at what is needed for capacity planning and other activities. The model also does not properly address what happens when the National Telecommunications and Information

Administration (NTIA) denies or times-out on a root zone change request. Although the NTIA has the reputation that they have never denied or have timed-out on a change request, but they can take other actions to achieve the same effect. Because the model does not address this issue, it leaves the process in an undefined state.

2. The JAS report analyzes the difficulty of carrying out the IANA function if there is a significant, extended outage of the Internet, and, on the basis of the dependency on email, suggests the IANA function should be provisioned with backup communications systems. This is a compound error in the threat model. First, there is not credible basis for assuming the Internet will suffer a significant extended outage. The document cited is a Business Roundtable report, which the SSAC does not accept as credible. Second, if the Internet were down an extended period of time, unless the IANA function were relevant to bringing it back up, the SSAC doubts that anyone would care whether the IANA function was operating.

3. The SSAC thinks that the report should examine scenarios where an emergency publication of a root zone is needed.

4. Comments on the Report's Recommendations

4.1 Documentation

The JAS report does not contain enough concrete documentation on how the root zone change process works, particularly with the introduction of the new automated Root Zone Management System. In this respect, the SSAC agrees with JAS report that better documentation is needed.

The SSAC acknowledges that documenting some pieces of the process may not be possible in enough detail for the JAS analysis due to extreme security and non-disclosure agreements for some of the steps. In this instance the SSAC thinks that the JAS report should at least acknowledge this point, and complement the lack of documentation with a risk analysis by saying that "enough people must always be under the appropriate non-disclosure agreements to restore that functionality." It is not a huge risk, but it is still a risk that should be raised.

4.2 More Formalization

A general thread throughout the JAS report recommendations seems to be that there should be a more formal approach to all the (sub-) processes involved (Recommendation 1,2,3,4). The SSAC welcomes these recommendations but would like to point out that they lack content and specificity. For example, Recommendation 4 asks for more training and certification, but it does not say what kind of training and certification is needed.

4.3 Reporting

In Section 7.1 the JAS report recommends formal monitoring on the risk of the Root Management process. The SSAC would like to see a recommendation for an extension of such monitoring in order to have enough data for a "holistic" capacity planning and modeling.

4.4 Service Level

Recommendations on service levels do not have to do with continuation and outages and security of IANA. It is more some interest "customers" of IANA might have and the need for expedited services.

5. Comments on Specific Points

Listed by page and item number, the SSAC provides the following comments:

Page 5, Item 2.1, Current "Manual" implementation:

- The SSAC suggests that "small, expert, and loyal staff" and "light workload" are pure judgment without relevance to the staff.
- What are the details to back up the following statement: "the root case of several historical errors"?
- What are the numerator and denominator and what is being measured in this statement: "very low error rate (less than 1%)"?

Page 6, Item 2.2, Future "Automated" implementation

- In the first paragraph are all errors related to rekeying?

Page 7, Item 2.4, Recommendations

Recommendation 1:

- What role is recommended for the Board's IANA Committee, the Risk Committee, or for the SSAC, if any?
- Concerning the risk of outage versus the risk of error a distinction should be made between what is intentional versus what is unintentional.

Recommendation 4:

- There should be a recommendation to include the two-person rule in travel policies and in other areas. In addition, where two-persons rules apply, recommendations should take into consideration efficiency, which will necessitate good cost accounting.

Recommendation 6:

- What is tolerable for an impact with no change to the root?

Recommendation 7:

- Recommendations should include the need to exercise regularly to increase the resilience of communications.

Recommendation 10:

- This is a good recommendation and the SSAC supports it.

Page 17, Item 5, Results

The number of transactions for one error occurrence may be a more understandable figure.

Page 17, Item 5.1

Lack of information at Modality of Historical Errors: How many are there from each category? What are the equations?

Page 17, Item 5.2

Factor Impacting Timeliness: The underlying model looks flawed.

Page 18, Item 5.4.1

Request Tracker Ticketing System (RT): Is that the best practice in place in the industry, e.g., nine hours per year? The SSAC suggests that hours-per-day has more significance.

Page 18, Item 5.4.2

Root Zone Management System (RZMS): Regarding the statement, "Finally, RZMS will interact directly with VeriSign using the Extensible Provisioning Protocol (EPP)." The SSAC thinks that there are two distinct parts with distinct characteristics.

Page 19, Item 5.4.4

The statement in this item is based on the Business Roundtable report, which the SSAC does not think is credible.

Page 20, Item 5.4.5

The SSAC does not consider the assumption in the statement, “99% availability… approximately 3.5 days a year” to be a helpful or most reliable model.

Page 20, Item 5.5

Dependence of Staff: Are these points relevant for consideration?

Page 20, Item 5.6

Dependence of physical location: ICANN had an exercise to see how well things work within the Los Angeles area, but concentration in a specific and possible risk area such as Los Angeles is relevant for further considerations.

Page 22, Item 6.1

Unintentional Human Error: The “Key” word should not be used in reference to an information entrance in order to avoid misinterpretation with “crypto key,” commonly used in this area.

Page 22, Item 6.2

Intentional Human Error/Insider Threat: The statement, "While it is extremely probable that errors output from ICANN/IANA would be caught by partners prior to implementation in the root zone file..." presumes that the "partners" will act in editing the zone in addition to sending proper information. However, previous root operators' in queries resulted in negative responses. This statement may be correct for VeriSign or perhaps for NTIA, but if that were the case, it would be better to not use "partners" in general.

6. Comments on the IANA Explanatory Memoranda

IANA published a response to the JAS recommendations, the "Explanatory Memoranda Regarding the Report 'IANA Process for Implementing Root Zone Change Requests – Review and Assessment of Risk Management Strategy and Comparison of Implementation Options.'"[3] The IANA document responds to the nine recommendations provided in the JAS report. The SSAC reviewed the IANA responses. It agreed with the responses to recommendations 2, 3, 4, 5, 6, 8, and 9. However, the SSAC had comments relating to recommendations 1 and 7, as follows:

Comments on IANA Response to Recommendation 1

In response to JAS recommendation 1, IANA says they have "clarified several critical questions of risk governance by clearly listing critical ICANN processes and systems in the ICANN Business Continuity plan and introducing a requirement limiting acceptable service downtime following a continuity event to a maximum of four hours." What is the basis for the four-hour threshold? IANA's activities are carried out primarily during normal business hours, so there is a general cessation of activity each evening until the next morning, and during weekends and holidays the cessation is two or more days. There is little value in setting the maximum too low and doing so increases cost and distracts from other priorities.

Comments on IANA Response to Recommendation 7

In response to JAS recommendation 7, "ICANN has procured GETS/WPS capabilities for critical employees and has distributed satellite phones strategically." The predicate for this JAS recommendation is a prolonged outage of the Internet. The claim that the Internet as a whole will be disrupted for an extended period of time is very suspect, and even if the Internet were to be down for an extended period of time, it is not clear that anyone would care whether the IANA function is operational unless the IANA function is critical to the restoration of the network. That case has not been presented, and it is not evident that any such connection exists. Therefore, it appears that the expense and distraction of the GETS/WPS capabilities are unnecessary.

[3] See <www.icann.org/en/reviews/iana/iana-root-zone-process-review-16jun10-en.pdf>.

7. Acknowledgments, Statements of Interests, and Objections and Withdrawals

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

7.1 Acknowledgments

The committee wishes to thank the following SSAC members and invited guests and members of the Root Scaling Study Team for their time, contributions, and review in producing this Comment.

Jaap Akkerhuis
Steve Crocker
Patrik Fältström
Jeremy Hitchcock
Ram Mohan
Ray Plzak
Vanda Scartezini

7.2 Statements of Interest

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

7.3 Objections and Withdrawals

There are no objections or withdrawals.