Summary Report of Public Comment Proceeding

Draft Framework for the Registry Operator to Respond to Security Threats

Publication Date:	11 September 2017
Prepared By:	Dennis Chang

Public Comment Proceeding	
Open Date:	14 June 2017
Close Date:	31 July 2017
Staff Report Due Date:	7 September 2017

Important Information Links
Announcement
Public Comment Proceeding
View Comments Submitted

Staff Contact:	Dennis Chang	**Email:**	dennis.chang@icann.org

Section I: General Overview and Next Steps

General Overview

On 14 June 2017, ICANN posted the Draft Framework for the Registry Operator to Respond to Security Threats for public comment. The deadline to receive public comments was 31 July 2017.

This public comment forum is intended to gather community feedback on the proposed Framework for the Registry Operator to Respond to Security Threats that has been a collaborative effort of the members of the Security Framework Drafting Team (SFDT) on behalf of the Registries Stakeholder Group (RySG), Public Safety Working Group (PSWG), Registrar Stakeholder Group (RrSG) and ICANN organization. The SFDT, consisting of representatives from registries, registrars, and the GAC PSWG, has collaborated with ICANN organization over the past two years to produce this draft document ("Framework"). The draft document has been reviewed by the RySG, RrSG, PSWG of the Governmental Advisory Committee (GAC), and no organization objected to or expressed concern with the draft.

At the time this report was drafted, six comments were submitted to the forum.

Next steps

ICANN organization is in the process of reviewing the comments it has received in collaboration with the SFDT to determine whether any changes need to be made to the proposed Framework. The final version of the Framework will then be publicly posted on the ICANN website for the benefit of the community.

Section II: Contributors

At the time this report was prepared, a total of six (6) community submissions had been posted to the forum. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III), such citations will reference the contributor's initials.

Organizations and Groups:

Name	Submitted by	Initials
Internet Society Venezuela	Ricardo Holmquist	ISOC
Registry Stakeholder Group	Stéphane Van Gelder	RySG
Business Constituency	Steve DelBianco	BC
Intellectual Property Constituency	Gregory S. Shatan	IPC
The Non-Commercial Stakeholders Group	Rafik Dammak	NCSG

Individuals:

Name	Affiliation (if provided)	Initials
R.R. KRISHNAA		RR

Section III: Summary of Comments

General Disclaimer: This section intends to summarize broadly and comprehensively the comments submitted to this public comment proceeding but does not address every specific position stated by each contributor. The preparer recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).

ICANN has received six (6) comments from the community on the proposed Framework for the Registry Operator to Respond to Security Threats.

For ease of reference, comments submitted will be organized by commenter.

Comments from R.R. Krishnaa:

1. Refer: Page No.2: Redirect name services for the domain name: The RO may adopt this process by aligning with CERT or any law enforcement agency. Prior permission from LEA (Law Enforcement Agency) or CERT will provide safety for taking actions.

2.. Refer: Page No.3: Take no action:

2a).. The first portion of the suggestion says that "RO may reach the conclusion that a referred matter does not constitute a security threat". It is submitted that RO may not decide whether a referred matter is a security threat or not. LEA or CERT or any other national body expertise in handling cyber threats may alone DETERMINE a threat as a security threat. RO may take action based on the advice of LEA or CERT.

2b).. The second portion of the suggestion says that "that the consequences of action outweigh the threat itself". This may also not be a right approach. It rather leads to more complications as action is not taken in the matter. The following options may be exercised:-

(i) A cautious approach to seek the advice of CERT or LEA and inform openly that the consequences of action outweigh the threat itself and seek advice on how to proceed in such cases.

(ii) RO may inform the originator/requester to contact CERT or LEA and submit their advice to RO. RO can safely take action on such advice of CERT or LEA.

3. Referring to Page No.4: This paragraph relates to the validity of the source of requests. Apart from its own sources, the RO may forward such requests to their national LEA or CERT and validate the authenticity and credibility of the requester.

4. Further it is submitted that if a RO receives a request relating to a different domain which is not in their management or control (for reasons such as the domains are under another RO), the RO who has received the request may inform the requester or originator to contact the relevant RO and provide the contact details of the relevant RO. Cases relating to "abuse" may not be left unaddressed for any reasons.

5. An "alternate action" is proposed: In case the requested action is not possible to implement due to technical feasibility, cost, or consequences of taking such action, the RO may inform the originator about any alternate action which is feasible and obtain the consent in writing to perform such action.

Comments from Ricardo Holmquist of ISOC Venezuela:

1. "If and when requests are categorized as "High Priority" and of a legitimate and credible origin, then, as soon as possible, and no later than 24 hours of acknowledging receipt, the Registry Operator can acknowledge the threat and communicate its planned steps to mitigate the security threat. When incidents are not categorized as "High Priority," the ROs are encouraged to respond within 24 hours with details of what they will be doing moving forward, or indicate that they will not take action. It is encouraged that ROs communicate the analysis of the threat to the requestor in order to clarify why they may or may not be taking further action or that mitigation should be handled through a different party".

2. The last page of the document should be rephrased or enhanced:

2a. Particularly where it currently states that the "Registry Operator *can* acknowledge..", it should say "RO *must* acknowledge" or even "RO *might* acknowledge", but the *can* seems to state permission to move ahead.

2b. Also "...ROs are encouraged to respond within 24 hours with details of what they will be doing moving forward, to include that they may be doing nothing..', uses language that seems to be permitting inaction by the RO, when it should be the least desirable option in most cases. I recommend concluding with "..moving forward.", the next phrase includes the "doing nothing" condition.

Comments from the Registry Stakeholder Group (RySG):

1. The Registries Stakeholder Group (RySG) welcomes the "Draft Framework for the Registry Operator to Respond to Security Threats" and highly appreciates the efforts by the members of the Security Framework Drafting Team (SFDT) that lead to a draft Framework supported by the different parties around the table.

2. The RySG is pleased to see that the deliberations within the SDFT have led to better insight and understanding among the parties involved of the possible actions and limitations for

Registry Operators when it comes to reacting on reported security threats. We hope that the Draft Framework paves the way for an improved relationship with the GAC PSWG, the GAC, and others.

3. The RySG wants to stress the importance of the voluntary and non-binding character of the Framework allowing Registry Operators to choose to take action considered appropriate after assessment of the reported threat. Registry Operators, as mentioned in the draft Framework, are not necessarily the best parties to address certain security threats.

Comments from the Intellectual Property Constituency (IPC):

1. The IPC appreciates the work of the Security Framework Drafting Team ("SFDT") in creating a thoughtful and comprehensive non-binding framework, addressing Registries' responses to notifications of security threats.

2. The IPC wishes to take this opportunity to draw attention to the significant overlap between online intellectual property infringement and security threats such as malware and phishing, which is supported by existing data and experience. There are several recent studies which highlight this overlap, noting that cybercriminals use well-known brands and popular copyrighted content, without authorization, in order to attract users, propagate malware, and carry out cybercrime activities. In particular:

3. A July 2016 study by the European Intellectual Property Office (EU IPO) finds that a number of business models supporting cybercriminal activity such as phishing make use of well-known brands in the email address and/or body of an email in order to deceive recipients into believing that the email comes from an authentic source. Another method uses a website spoofed to look like a legitimate site, in order to deceive users to disclose bank accounts and other personal data.

4. A recent example of this activity, demonstrating its applicability to the domain name space, involves Microsoft's enforcement efforts against the notorious hacking entity known as Fancy Bear, which had made illegitimate, infringing use of Microsoft's brands to carry out their security threats. Microsoft was recently successful in seizing control of hundreds of domain names referencing their brands, in order to disrupt Fancy Bear's cybercriminal network.

5. This strategy, highlighting the important link between security threats and cybersquatting, is not new. Microsoft has previously launched similar actions to take control of domains used in the propagation of Zeus and Ruckstock botnets.

6. In November 2016, Fairwinds Partners published details of their analysis of typosquatting activity, which identified a link between typo domains owned by squatters and malware. The study focused on the top 50 brands (excluding those whose names were based on descriptive terms, or which weren't associated with houses of brands) with names comprising 6 characters or more. The study found that amongst typo domains owned by squatters infringing these brands, 39% of them contained malware, phishing and ransomware and/or involved affiliate fraud.

7. A study by RiskIQ and the Digital Citizens Alliance also found that amongst a sample of 800 sites dedicated to distributing infringing movies and TV shows, one out of every three contained malwares. As such, consumers are 28 more times likely to get malware from

visiting a content theft site than visiting a licensed provider. Merely visiting such sites may place a consumer at risk, since malware is often delivered via “drive-by downloads”, invisibly downloading malware to a user’s computer without the user clicking on any link. The majority of malware from these sites took the form of Trojans to spy on the consumer’s computer, or adware to co-opt the consumer’s computer into advertising fraud schemes.

8. One subset of data that is important to note is the ratio of domains which are registered initially for purposes linked to security threats, versus those that are compromised following their registration. For example, a recent report by the Anti-Phishing Working Group (APWG) noted that the overall ratio between domains that were registered for phishing purposes and those that were compromised by phishers is about 49% to 51%. However, the APWG’s analysis revealed that certain registrars had a rate which far exceeded that, indicating a high volume of malicious registrations. It is important to understand the factors contributing to that, and how better policies and practices amongst registrars can reduce the number of malicious registrations, and thus reduce security threats as well.

9. This important data demonstrates the need to better understand how security threats are propagated via various types of abusive activity (as that term is used in registries and registrars’ contractual obligations to ICANN), including intellectual property infringement. More data would be helpful, as well as a recognition that addressing intellectual property infringement, as a species of abuse, is an integral part of carrying out ICANN’s mission to ensure the stable and secure operation of the DNS.

10. In order to track and understand the various threats, IPC suggests that registries should begin collecting and sharing data, which can form the basis of future research and threat-mitigation procedures. Establishment of a cross-registry security threat depository system where reported data will be shared and accessed by approved members such as law enforcement authorities, registries, cybersecurity firms, private investigators, brand owner representatives, etc. would be beneficial to contracted parties, consumers and as others having an interest in abuse mitigation and ensuring the stable and secure operation of the DNS. This data should not only include security threat data but also data about other abuse complaints.

11. Leading on from that, the IPC also wishes to note that the Framework may serve as a useful template to help promote transparency and effectiveness in registrars’ and registries’ responses to other types of abuse complaints. We anticipate that many of the points addressed in the Framework would be applicable to responses to IP-related abuse, including suggested actions which could be taken in response to an abuse complaint.

Comments from the Business Constituency (BC):

1. This is a potentially important next step in enhancing security and stability of the DNS through Registry Operator (“RO”) level procedures for handling security threats and abuse within the Domain Name System (“DNS”). The BC has a long and well-documented history of supporting safeguards and procedures against DNS abuse.[2] While we commend the drafters for a sensible approach to laying the groundwork for what may ultimately become a more robust best practices program, we recommend the following changes and additions to the Draft:

More definitions. For example, the Draft refers to "significant threat of disruption to the

DNS" and, without more, it is difficult to understand what falls within that bucket, or for an RO to truly adhere to a uniform best practice to address "significant threat of disruption to the DNS";

Direct call to action. The Draft often “encourages” or suggests ROs “may choose” to take certain actions. Although this framework is meant to be voluntary and non-binding, in order to be produce any sort of uniform best practices, it should provide a more direct call to action, by using more direct language (e.g., “should” or “will”). As a voluntary and non-binding framework, those who choose to subscribe should have a clear roadmap of the outlined best practice.

Content. The Draft discusses how ROs should evaluate the content of abuse reports. This may be a difficult exercise when there is no uniformity to the substance and format of abuse reports.

See other BC Positions and comments:

- http://www.bizconst.org/assets/docs/positions-statements/2016/2016_05may_bc-commenton-safeguards-to-mitigate-dns-abuse.pdf (Comment on New gTLD Program Safeguards to Mitigate DNS Abuse)
- http://www.bizconst.org/assets/docs/positionsstatements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gtld%20base%20registry%20agreement%20final.pdf (Comment on Proposed Amendments to Base New gTLD Registry Agreement);
- http://www.bizconst.org/assets/docs/positionsstatements/2017/2017_05May_19%20BC%20Comment%20on%20CCTRT%20recommendations.pdf (Comment on Competition Consumer Trust & Consumer Choice Review Team Draft Report of Recommendations for New gTLDs);
- http://www.bizconst.org/assets/docs/positionsstatements/2017/2017_05May_22%20BC%20reply%20to%20questionnaire%20on%20new%20gTLD%20Subsequent%20Procedures.pdf (Reply to Questionnaire from new gTLD Subsequent Procedures PDP)

3. We recommend that the drafters be directed to work together with relevant ICANN Security staff to produce addendums to the Draft that contain suggested language for abuse reports. These “templates” could be published as part of any public reporting interface for abuse, making the reporting process and digestion of those reports more predictable and uniform in both submission and response by ROs.

4. Once the Draft is revised to include more direct, concrete, and implementable action items to be considered a “best practice”, the BC recommends that a next step should be ICANN’s formulation of an incentive program to encourage ROs to subscribe to the resulting best practices. As noted in a previous BC comment:

5. The BC supports enabling ICANN to reduce registry fees to incentivize Registry Operators to engage in practices that help mitigate the proliferation of abusive domain names in their TLDs, and thereby support and enhance internet security and contribute to a healthy domain name ecosystem. There is strong precedent for ICANN to unilaterally reduce contracted party fees to promote such good behavior. For example, at various times in the past, ICANN unilaterally reduced fees for registrars that adopted a new RAA, ended “drop catching,” and stopped “domain tasting.”

6. With an ICANN supported and incentivized best practices document/program, we are sure

to see more support through increased and documented RO subscription.

7. While the BC supports all the efforts that led to and formed the Draft, it believes the Draft requires some revision to truly become the basis for a voluntary RO best practice program that addresses security threats in the DNS. Without more definition, direct call to action, or uniform abuse reporting mechanisms, it is hard to imagine how best practices emerge from the Draft -- leaving us with a mere list of well-documented possible/sensible approaches for handling security threats in the DNS.

8. It is also hard to see a path beyond this Draft without ICANN's full support via an incentive program. As such, we encourage the drafters and ICANN to take the logical next steps in this process to ensure that the hard work to-date is not wasted and that a best practices program for handling security threats in the DNS can emerge from all of this work.

Comments from the Non-Commercial Stakeholders Group (NCSG):

1. We support ICANN effort to address global security threat issue with outlining the response recommendation to threat notifications.

2. Since the following examination of threat report is identified in the Framework, we strongly suggest including a recommendation on Responsible Threat Disclosure to be included in the document: "Each RO should scrutinize, question or otherwise inquire about the legitimacy of the origin of a request, in accordance with their own internal policies and processes."

3. We have seen a broad variation in handling security threat reports, varying from constructive actions addressing the issues to punishment of the reporting party. Benefits of responsible threat submission are obvious.

4. In this context, it is important to underline benefits and importance of responsible threat disclosure. We request recommendation to extend goodwill and not cause harm to the reporting party whenever possible:

- an easy way to report security threats and violation
- encrypted ways of communication
- option of anonymous submission

5. "With respect to the safeguards regarding security checks, the NGPC considered that the comments in opposition raise important questions about the costs and timing of implementing this measure, and the scope and framework of the security checks.

6. The NGPC is mindful that there are various ways a registry operator could implement the required security checks, and has taken these concerns into consideration in its response to the GAC's advice. The NGPC's response directs ICANN to solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality.

7. The proposed implementation of the GAC's advice is phased to account for the

commenters' concerns. The proposed language in the PIC Specification will provide the general guidelines for what registry operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks."

- Providing specific examples of the most common threats

- Connecting listed actions to the use cases

8. Also request for "respecting privacy and confidentiality" is not clearly addressed within the proposed Framework.

9. Overall, we recognize the Framework as very welcome initiative. At the moment the Framework is not ready for publication, but is a work in progress that needs more elaboration and clarification. The information in insufficient within the intended scope.

10. We thank SFDT for conducting a public comment for broader community feedback prior to finalization of the Framework, even though it was not required. We are looking forward to addressing the points of this comment.

Section IV: Analysis of Comments

General Disclaimer: This section intends to provide an analysis and evaluation of the comments submitted along with explanations regarding the basis for any recommendations provided within the analysis.

The SFDT appreciates all comments and suggestions added to the public forum for the proposed Framework for the Registry Operator to Respond to Security Threats. The SFDT has reviewed all comments and offers the following analysis. The analysis below is organized by the type of comments and topics of the draft Security Framework.

1. Comments in support of the Security Framework and the work of the SFDT

The SFDT appreciates the following statements of support for the Security Framework and the work methodology used by the SFDT. The SFDT found that collaborative work method proved to be efficient and effective.

- The NCSG stated: We thank SFDT for conducting a public comment for broader community feedback prior to finalization of the Framework, even though it was not required.
- The RySG stated: The Registries Stakeholder Group welcomes the “Draft Framework for the Registry Operator to Respond to Security Threats” and highly appreciates the efforts by the members of the Security Framework Drafting Team that lead to a draft Framework supported by the different parties around the table.
- The RySG stated: The RySG is pleased to see that the deliberations within the SDFT have lead to a better insight and understanding among the parties involved of the possible actions and limitations for Registry Operators when it comes to reacting on reported security threats. We hope that the Draft Framework paves the way for an improved relationship with the GAC PSWG, the GAC, and others.
- The IPC stated: The IPC appreciates the work of the Security Framework Drafting Team in creating a thoughtful and comprehensive non-binding framework, addressing Registries’ responses to notifications of security threats.
- The BC stated: This is a potentially important next step in enhancing security and stability of the DNS through Registry Operator level procedures for handling security threats and abuse

within the Domain Name System. The BC has a long and well-documented history of supporting safeguards and procedures against DNS abuse.

- The NCSG stated: We support ICANN effort to address global security threat issue with outlining the response recommendation to threat notifications.
- The IPC stated: The IPC wishes to note that the Framework may serve as a useful template to help promote transparency and effectiveness in registrars' and registries' responses to other types of abuse complaints. We anticipate that many of the points addressed in the Framework would be applicable to responses to IP-related abuse, including suggested actions which could be taken in response to an abuse complaint.
- The NCSG stated: We have seen a broad variation in handling security threat reports, varying from constructive actions addressing the issues to punishment of the reporting party. Benefits of responsible threat submission are obvious.

2. Comments regarding the scope of the Security Framework

The SFDT appreciates the following comments to reinforce the scope of the Security Framework project.

- The RySG wants to stress the importance of the voluntary and non-binding character of the Framework to allow for Registry Operators to choose to take actions considered appropriate after assessment of the reported threat. Registry Operators, as mentioned in the draft Framework, are not necessarily the best parties to address certain security threats. Framework will retain the clear language for the voluntary and non-binding nature of this work.
- The NCSG considered that the comments in opposition to safeguards regarding security checks raise important questions about scope and framework, as well as the costs and timing of implementing the measures.
- The NCSG is mindful that there are various ways a registry operator could implement the required security checks, and has taken these concerns into consideration in its response to the GAC's advice. The NCSG response directs ICANN to solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality.
- The proposed implementation of the GAC's advice is phased to account for the commenters' concerns. The proposed language in the PIC Specification will provide the general guidelines for what registry operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks.

The SFDT being a team consisting members from registries, registrars and PSWG (GAC) is keenly aware of the limited scope of this project and the Security Framework should reflect this accurately. It should be noted that the SFDT engaged in lengthy specific conversation with regards to likely cost implications of the Security Framework; particular emphasis was placed on how overly onerous requirements could be of particular disadvantage and financial burden to smaller entities. Deference is therefore paid to the multitude of shapes and sizes of ROs involved, and in particular the application of the RO's own policy. This ensures that no RO should be obligated to act in a manner that is either objectively or subjectively unreasonable.

3. Comments providing general information about the Security Threats

The SFDT appreciates the following comments offering general insights and information to the SFDT.

- The IPC draws attention to the significant overlap between online intellectual property infringement and security threats such as malware and phishing, which is supported by existing data and experience. There are several recent studies which highlight this overlap, noting that cybercriminals use well-known brands and popular copyrighted content, without authorization, in order to attract users, propagate malware and carry out cybercrime activities.

- The IPC points out a July 2016 study by the European Intellectual Property Office (EU IPO) finds that a number of business models supporting cybercriminal activity such as phishing make use of well-known brands in the email address and/or body of an email in order to deceive recipients into believing that the email comes from an authentic source. Another method uses a website spoofed to look like a legitimate site, in order to deceive users to disclose bank accounts and other personal data.
- The IPC provides a recent example of this activity, demonstrating its applicability to the domain name space, involves Microsoft's enforcement efforts against the notorious hacking entity known as Fancy Bear, which had made illegitimate, infringing use of Microsoft's brands to carry out their security threats. Microsoft was recently successful in seizing control of hundreds of domain names referencing their brands, in order to disrupt Fancy Bear's cybercriminal network. This strategy, highlighting the important link between security threats and cybersquatting, is not new. Microsoft has previously launched similar actions to take control of domains used in the propagation of Zeus and Ruckstock botnets.
- The IPC noted that in November 2016, Fairwinds Partners published details of their analysis of typosquatting activity, which identified a link between typo domains owned by squatters and malware. The study focused on the top 50 brands (excluding those whose names were based on descriptive terms, or which weren't associated with houses of brands) with names comprising 6 characters or more. The study found that amongst typo domains owned by squatters infringing these brands, 39% of them contained malware, phishing and ransomware and/or involved affiliate fraud.
- The IPC points out a study by RiskIQ and the Digital Citizens Alliance also found that amongst a sample of 800 sites dedicated to distributing infringing movies and TV shows, one out of every three contained malwares. As such, consumers are 28 more times likely to get malware from visiting a content theft site than visiting a licensed provider. Merely visiting such sites may place a consumer at risk, since malware is often delivered via "drive-by downloads", invisibly downloading malware to a user's computer without the user clicking on any link. The majority of malware from these sites took the form of Trojans to spy on the consumer's computer, or adware to co-opt the consumer's computer into advertising fraud schemes.
- The IPC stated: One subset of data that is important to note is the ratio of domains which are registered initially for purposes linked to security threats, versus those that are compromised following their registration. For example, a recent report by the Anti-Phishing Working Group (APWG) noted that the overall ratio between domains that were registered for phishing purposes and those that were compromised by phishers is about 49% to 51%. However, the APWG's analysis revealed that certain registrars had a rate which far exceeded that, indicating a high volume of malicious registrations. It is important to understand the factors contributing to that, and how better policies and practices amongst registrars can reduce the number of malicious registrations, and thus reduce security threats as well.
- The IPC stated: This important data demonstrates the need to better understand how security threats are propagated via various types of abusive activity (as that term is used in registries and registrars' contractual obligations to ICANN), including intellectual property infringement. More data would be helpful, as well as a recognition that addressing intellectual property infringement, as a species of abuse, is an integral part of carrying out ICANN's mission to ensure the stable and secure operation of the DNS.

The SFDT appreciates the in-depth research presented for consideration, and accepts there exists a correlation between sites that present material that may be in breach of intellectual property rights, and the presence of malware and other technical abuse of the DNS. However, in such instances, the in-scope security threat is represented by the malware and not the other material that may be presented in connection with a particular domain name. We remain of the belief that such IP related matters remain out-of-scope of the endeavor.

4. Comments with suggestions for Subsequent work
The SFDT appreciates the following comments from various groups with encouragements for the SFDT to continue with additional work.

- The BC stated: Finally, once the Draft is revised to result in more direct, concrete, and implementable action items to be considered a “best practice”, the BC recommends that a next step should be ICANN’s formulation of an incentive program to encourage ROs to subscribe to the resulting best practices. The BC supports enabling ICANN to reduce registry fees to incentivize Registry Operators to engage in practices that help mitigate the proliferation of abusive domain names in their TLDs, and thereby support and enhance internet security and contribute to a healthy domain name ecosystem.
  - Recommendations for creation of incentive programs or fee reduction are out of scope for the voluntary Security Framework. The SFDT have endeavored to to ensure the Framework is applicable to as many registry operators as possible. It is hoped that this focus on universality will result in the greatest number of ROs intending to follow the example of the framework.
- The IPC stated: In order to track and understand the various threats, IPC suggests that registries should begin collecting and sharing data, which can form the basis of future research and threat-mitigation procedures. Establishment of a cross-registry security threat depository system where reported data will be shared and accessed by approved members such as law enforcement authorities, registries, cybersecurity firms, private investigators, brand owner representatives, etc. would be beneficial to contracted parties, consumers and as others having an interest in abuse mitigation and ensuring the stable and secure operation of the DNS. This data should not only include security threat data but also data about other abuse complaints.
- The BC stated: Content. The Draft discusses how ROs should evaluate the content of abuse reports. This may be a difficult exercise when there is no uniformity to the substance and format of abuse reports. As such, we recommend that the drafters be directed to work together with relevant ICANN Security staff to produce addendums to the Draft that contain suggested language for abuse reports. These “templates” could be published as part of any public reporting interface for abuse, making the reporting process and digestion of those reports more predictable and uniform in both submission and response by ROs.
  - The SFDT appreciates the suggestion, however must note that the Security Framework is only concerned with the response to identified security threats, and not the form in which such security threats are reported or received. The SFDT remains supportive of supplementary and separately constituted endeavors to further review such matters.

The SFDT’s task is to draft the framework, within the confines of the scope as set by the NGPC commitment. We have welcomed the opportunity to work closely with our industry colleagues, and acknowledge that there may be future, separately constituted endeavors, which may expand upon the work of the SFDT, once the team has completed its task. Whereas we appreciate the suggestion presented regarding subsequent work, they remain, for the Purposes of the Security framework, to be out of scope.

5. Comments with a recommendation for additions to current version
The following comments recommends addition to the Security Framework before its initial publication. The SFDT has reviewed the comments and offer the following responses.

- In response to RR’s proposal for an “Alternate Action” in case of the requested action is not possible to implement due to technical feasibility or costs or consequences that could occur on taking such action. RR suggests the RO may inform the originator about any alternate action which is feasible and obtain the consent in writing to perform such alternate action.

  - Responses to identified security threats, other than those mandated by a court order of a suitable jurisdiction, are at the discretion of the RO and the application of their policy. Neither the consent of the originator nor a RO taking an action in all instances, in particular where it is not technically feasible, is required. The Security Framework encourages the most relevant and timely action possible in any situation, but regardless the RO still may not be in a position, or may not be considered to be the most appropriate party to carry out an action.

- In response to the BC's comment that the Draft requires some revision to include more definitions, direct call to action, and reporting mechanism to truly become the basis for a voluntary RO best practice program that addresses security threats in the DNS.
  - The mechanisms described in the comment are considered to be out of scope. The SFDT were limited to the confines of the NGPC commitment. We believe that the Security Framework is a grounding document, and the team continues to be supportive of other separately constituted and related endeavors, which may supplement the Security Framework, but which nonetheless lie beyond the scope of this document.
- In response to NCSG's request for "respecting privacy and confidentiality" that is not clearly addressed within the proposed Framework, the SFDT, although noting that Privacy and confidentiality was a guiding principle throughout the drafting process, accepts that more explicit clarification may be of benefit and the SFDT plans to add a statement to address this in the initial publication.
- In response to the NCSG's comment that while the Framework as very welcome initiative, at the moment the Framework is not ready for publication, but is a work in progress that needs more elaboration and clarification and the information is insufficient within the intended scope. The SFDT acknowledges the critique, however has engaged in in-depth conversation, with input from registries, registrars and representatives of law enforcement (PSWG), so as to ensure that all matters, as contained within the NGPC commitment have been reviewed and are adequately addressed in the framework.
- In response to the NGSC's suggestion to providing specific examples of the most common threats and connecting listed actions to the use cases, the SFDT specifically decided against the insertion of specific examples, and related responses. Such an approach was grounded, to an extent on a lack of suitable examples available for inclusion; however, ultimately we felt it more appropriate to defer to the individual Registry Operator's interpretation and policy. SFDT appreciates the comments, but as security threats evolve, so too will Registry policies and responses to the same. This is one reason why the SFDT chose not to include enumerated examples of Security Threats, because they are, by their nature, ever-changing.

6. **Comments recommending changes to current version**

The SFDT appreciates the following recommendations and requests for specific changes to the registry operators responding the reported security threats. In general, the Security Framework is limited and bound to its scope only able to address those suggestions that are within scope. However, the SFDT has discussed and considered all recommendations and addressed them individually below.

- In response to the IPC's suggestion that registries should begin collecting and sharing data, which can form the basis of future research and threat-mitigation procedures and to establish a cross-registry security threat depository system where reported data will be shared and accessed by approved members, the SFDT believes this is out-of-scope for the current Security Framework work.
- In response to RR's suggestion to be aligning with CERT or any law enforcement agency on redirecting name services, the Security Framework specifically encourages all ROs to liaise with law enforcement agencies.

- In response to RR’s recommendation that ‘no action’ is not a suitable option and that ROs should seek the advice of CERT or LEA, as it is only the LEA or CERT that may decide if a matter is a security threat or not, the SFDT respectfully disagrees with RR. RO’s are encouraged to liaise with the CERT and LEA, but such interactions are not definitive, and unless backed by a valid Court Order or equivalent, the course of action chosen, including to ‘take no action’ ultimately is at the discretion of the RO.
- In response to RR’s suggestion for RO to receive prior permission from LEA (Law Enforcement Agency) or CERT before taking actions the SFDT again respectfully disagrees with RR. A RO is not required to seek the advice or permission of any party, prior to taking any such action. Unless a RO is in receipt of a valid Court Order, it is the sole decision of the RO to take any action or actions as they see fit, with due regard their own stated policies. The RO is strongly encouraged to liaise with LEAs, but permission is not required.
- In response to RR’s comment that RO should not decide whether a referred matter is a security threat or not to take action, but that only a LEA, CERT, or any other national body may alone DETERMINE a threat as a security threat for a RO to take action based on the advice of LEA or CERT, RO is encouraged to liaise with organizations with expertise in security threats, but the SFDT respectfully disagree that the RO is “required” to act on the instruction of any LEA or CERT, unless such an instruction is duly required by a valid Court Order.
- In response to RR’s comment that if a RO receives a request relating to a different domain which is not in their management or control (for reasons like such domains come under another RO), the RO who has received the request may inform the requester or originator to contact the relevant RO and provide the contact details of the said relevant RO, such referrals are out of scope for the Security Framework.
- In response to RH’s suggestion that the language in the document should be rephrased or enhanced to say replace "RO must acknowledge" rather than "Registry Operator can acknowledge.", the SFDT specifically decided upon the use of non-mandatory language. This ensures that, although all RO’s are encouraged to act in line with steps envisaged by the Security Framework, it is acknowledged that not all action noted may be suitable for a particular RO (local laws, or differing policy of that RO). The language chosen therefore ensures that implementing the Security Framework, does not expect specific ‘required’ courses of action, more so guidance on achieving an ultimate goal (i.e. a valid and strong response to an identified security threat).
- In response to the BC comments on the direct call to action to use more direct languages such as “will” rather than “encourage,” it should be noted that the Security Framework is a voluntary and non-binding framework and therefore language that suggests mandatory actions are not used.
    - See previous response regarding the decision to not use Mandatory Language.
- In response to NCSG’s suggestion to include “Each RO should scrutinize, question or otherwise inquire about the legitimacy of the origin of a request, in accordance with their own internal policies and processes” on Responsible Threat Disclosure, it should be noted that the Framework recommends that credibility of sources should be reviewed by the individual RO and the concept of legitimacy is encompassed in such a recommendation.
- In response to NCSG’s requests to extend goodwill and not cause harm to the reporting party whenever possible by providing an easy way to report security threats and violation, encrypted ways of communication and option of anonymous submission, the SFDT thanks the NCSG for bringing this previously undiscussed matter to our attention; the SFDT has decided to table this matter for further discussion in the near future, and we shall consider the applicability of this matter to the scope of the Security Framework, and where appropriate, as a result, any subsequent additions the Security Framework as we may see necessary.