ABUSE/COMPLIANCE SUBGROUP DRAFT 10 SEPT 2019

FINDINGS

WORLD SSR THREAT

- **MALWARE**
- **DIGITAL CERTIFICATE FRAUD/**
- **PHISHING**
- **BUSINESS EMAIL COMPROMISE**
- **SCAMS**
- **BOTNETS**
- **SPAM**
- **DDOS**

BIG GAP: WORLD THREAT & ICANN ACTION

NEW GTLD ABUSE
REGISTRAR ACCREDITATION AGREEMENT
SSAC
GAC & OTHER STAKEHOLDERS
REVIEWS
DAAR
ICANN COMPLIANCE

RECOMMENDATIONS:

1) COMPLIANCE - THE BOARD AND ICANN ORG SHOULD FUNDAMENTALLY CHANGE THE COMPLIANCE REGIME.

· COMPLIANCE MUST BE EMPOWERED
· COMPLIANCE SHOULD PARTNER WITH COMPLAINANTS AND SERVE THE PUBLIC INTEREST.

2) ABUSE DEFINITIONS & REPORTING - ICANN BOARD AND ICANN ORG SHOULD OVERHAUL ICANN'S APPROACH TO DNS ABUSE DEFINITIONS, TRACKING AND REPORTING.

· IMPLEMENT CCT REVIEW RECOMMENDATIONS
· USE THE CURRENT DNS ABUSE DEFINITION PLUS CONVENTION ON CYBERCRIME.
· ICANN SHOULD ESTABLISH A SINGLE COMPLAINT PORTAL FOR ALL COMPLAINTS
· IMPROVE COMPLAINT REPORTING AND SECURITY THREAT REPORTING.

3) POLICIES AND AGREEMENTS WITH CONTRACTED PARTIES – ADOPT NEW ONES THAT MEANINGFULLY IMPACT MITIGATION OF DNS ABUSE AND SECURITY THREATS.

· UPDATE KEY POLICIES AND PRACTICES IMPACTING SECURITY THREAT MITIGATION.
· INCENTIVIZE CONTRACTED PARTIES TO MITIGATE ABUSE AND SECURITY THREATS.

· INCORPORATE MEASURES TO MITIGATE "DNS ABUSE" AND "SECURITY THREATS" IN AGREEMENTS WITH CONTRACTED PARTIES,
· INSTITUTIONALIZE TRAINING AND CERTIFICATIONS FOR CONTRACTED PARTIES AND KEY STAKEHOLDERS

FINDINGS

Global Threats to SSR

Since its founding, ICANN has had a remit to help ensure the security, stability and resiliency of the Internet's unique identifier systems. While there's a strong record of ICANN's policies and actions supporting competition and growth in the domain space, ICANN's record on supporting impactful security, stability and resiliency measures is deeply insufficient.

Globally, there has been an increased risk of attacks against critical infrastructures, malicious political interference, and a range of cybercrimes. ICANN's failure to fulfill responsibilities relating to domain name system (DNS) security, stability and resiliency runs the risk of malicious actors capitalizing on this failure. Damages associated with cybercrime globally are projected to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015[1]. The *2019 Official Annual Cybercrime Report* notes that "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined."[1]

The SSR2 team identified a significant upward trend in multiple examples of abusive behaviors that can and often do leverage the DNS. Cybercriminals and other threat actors capitalize on identifiable gaps in DNS security measures currently in place. Relevent trends especially have been observed since the first SSR Review Team report was adopted by the Board in 2012. Examples connected to the DNS to varying degrees include:

- Malware - from 2016 to 2018, the number of unique URLs recognized as malicious by antivirus software more than doubled to 554,159,6213[2], and mobile malware attacks nearly doubled from 2017 to 2018 to over 116 million[3].
- Digital Certificate Fraud - APWG reports that phishers are increasingly using digital certificates to make attacks look legitimate and to defeat browser fraud detection warnings.[4] Due to ICANN actions, SSL certificate administration no longer has access to

[1] Cybersecurity Ventures Official Annual Cybercrime Report, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] Kaspersky Security Bulletin, https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/

[3] Mobile Malware Evolution 2018, Victor Chebyshev, https://securelist.com/mobile-malware-evolution-2018/89689/

[4] APWG Phishing Activity Trends Report 3rd Quarter 2018, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf

domain name registration data and can't use the domain name ownership records that ICANN is charged with coordinating to validate domain name ownership. PhishLabs determined that half of all phishing sites use SSL encryption, which can fool users into thinking that a site is safe to use, for example, by virtue of the green lock symbol that appears in the browser address bar when SSL encryption is enabled. Some of the increase comes from phishers adding HTTP encryption to their phishing sites – a technique that turns a security feature against the victims.[5]

- Phishing - APWG reported that phishers are registering domain names directly to perpetrate fraud, and that the methods of phishing attacks have become more effective and harder to detect. "Phishers are increasingly using web page redirects as a way of hiding their phishing sites from detection. When victims click on links in phishing emails, redirects take the user on an unwitting journey through other sites before arriving at the phishing site itself. And then once the victim submits his or her credentials, still more redirects make take the victim to yet another domain."[6]
- Business Email Compromise - The US FBI Internet Crime Center reported a 136% increase in identified global exposed losses from 2016 to 2018 resulting from Business Email Compromise, affecting all 50 United States and 150 countries worldwide. From October 2013 to May 2018, the FBI documented a multi-billion-dollar growth in BEC, which often involves fraudulent registration of domain names that are deceptively similar to one of the targeted parties.[7]
- Scams - The Australian Competition and Consumer Commission (ACCC) ScamWatch reported a near doubling in losses from scams in roughly the last three years, rising to AU$11.8 million in losses in 2019.[8] Domain names used to perpetrate online scams very typically infringe on brand or business name. These names are registered by the scammer with little or no controls over the volumes of similar names the scammer can register and limited access to information that investigators can use to identify the criminal actors.
- Botnets -- In 2017, Spamhaus DBL listed 50,000 botnet controller domain names registered and set up by cybercriminals for the sole purpose of hosting a botnet controller. More than 25% of these registered botnet domain names have been registered through a single registrar, Namecheap.[9] In 2018, Spamhaus listed 103,503

---

[5] 49 Percent of Phishing Sites Now Use HTTPS, PhishLabs blog by Elliot Volkman on Dec 6, '18, https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https

[6] Phishing Activity Trends Report

[7] Business E-Mail Compromise The 12 Billion Dollar Scam, Federal Bureau of Investigations Public Service Announcement, https://www.ic3.gov/media/2018/180712.aspx

[8] ScamWatch, Australian Competition and Consumer Commission, https://www.scamwatch.gov.au/about-scamwatch/scam-statistics

[9] Spamhaus Botnet Threat Report 2017, https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017

botnet controller domain names, a 106% increase. Namecheap remained the most abused registrar, with a 220% increase in registered botnet controller domain names.[10]

- Spam - Spam is the preferred delivery infrastructure for phishing, malware and other DNS-related threats. The average daily spam volume was 416.04 billion as of August 2019.[11] "No matter how much the threat landscape changes, malicious email and spam remain vital tools for adversaries to distribute malware because they take threats straight to the endpoint. By applying the right mix of social engineering techniques, such as phishing and malicious [domain name/URL] links and attachments, adversaries need only to sit back and wait for unsuspecting users to activate their exploits."[12]
- DDOS Attacks - Distributed denial of service (DDoS) attacks increased 40% from mid-2017 to mid-2018.[13] DDoS maximum attack size increased globally by 174% in the first half of 2018 over the same period in 2017, and the largest attack ever recorded -- *1.7 Tbps*[14] -- struck a large North American service provider in February 2018.[15] Because everything from businesses and goverment agencies to our basic infrastructure are dependent on uninterrupted DNS-related services, unmitigated DDoS attacks are increasingly harmful. DDoS attacks also have become more complex and multi-vector attacks are now the most commonly employed. Verisign reported 52% of their attacks recorded in the second quarter of 2018 were multi-vector attacks.[16] Additionally, the "internet of things" (IoT) is a growing concern for DDoS attacks because these connected devices are easy targets and they continue to proliferate. The number of connected devices was 27 billion in 2017 and is predicted to reach 125 billion by 2020.[17]

Gaps: World Threat & ICANN Action

In our review of ICANN's activities, we found that the publications and statements from ICANN Org have consistently understated or omitted the impact of systemic abuse of the DNS and its use as a platform for launching systematic attacks on individual and organizational systems worldwide.

---

[10] Spamhaus (specific webpage URL needed), https://www.spamhaus.org/

[11] Cisco Talos Intelligence Group, https://www.talosintelligence.com/reputation_center/email_rep

[12] Cisco 2018 Annual Cybersecurity Report, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

[13] H1 2018 DDOS Trends Report, Corero, https://info.corero.com/report-2018-half-year-ddos-trends-report-download.html

[14] Tbps stands for "Terabytes per second" and refers to a data transmission rate equivalent to 1,000 gigabytes, or 1,000,000,000,000 bytes per second.

[15] Entering the Terabit Era: Get Ready For Bigger DDoS Attacks, by Kevin Whalen, September 5, 2018, https://www.netscout.com/blog/entering-terabit-era-get-ready-bigger-ddos-attacks

[16] Verisign blog, Q2 2018 DDOS Trends Report: 52 Percent of Attacks Employed Multiple Attack Types, September 27, 2018, https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types/

[17] Getting the Network Ready to Meet IoT Expectations, NETSCOUT, February 28, 2018, https://www.netscout.com/blog/getting-network-ready-meet-iot-expectations

New gTLD Abuse - In 2010 and in anticipation of the expansion of the gTLD program, the ICANN community prepared a memorandum describing measures to mitigate malicious conduct in the new TLD program.[18] The published version of the memorandum included recommendations for vetting registry operators, but the implementation of background checks for criminal or malicious activity was limited. It also recommended that registries name and define registry-level abuse contacts and procedures but to date, no uniform or formal procedures are available or enforced, thus adversely impacting registry-level abuse mitigation. The memorandum further recommended the centralization of access to zone files but as of now, no consistent access to zone files has been established. Ongoing problems accessing zone file data via ICANN's Centralized Zone Data Service (CZDS) have been reported, and this continues to hamper security mitigations, investigations and research. Zone file data is used to identify newly resolving domain names that may be used in cyber attacks, including those noted above. Problems include registries failing to approve and provide access to zone data for legitimate users, registries failing to renew access to zone data for legitimate users, and registries failing to provide daily zone file data.[19]

Registrar Accreditation Agreement - Law enforcement, governments, security communities, and commercial and user interests groups all argued for contractual obligations to mitigate abuse during the deliberations of the 2013 Registrar Accreditation Agreement (RAA).[20] The few measures that survived the closed negotiations between ICANN Org staff and registrars. were significantly weakened. As of now, contracts do not include any language or terms specifically addressing systemic abuse and obligations of registrars in this regard. From reports, it is evident that some accredited registrars established a practice to process domain registrations by the thousands that are used for many of the criminal activities highlighted earlier. Alpnames, among the most egregious registrar as highlighted by the CCT Review report, offered cheap bulk registrations and at times over 80% of its portfolio was identified as abusive domains.[21] ICANN Compliance failed to address this ongoing, systemic abuse.[22] After ICANN became aware of the "discontinuance of [Alpnames] operations," ICANN Compliance de-accredited it and simply transferred the abuse-laden portfolio to other registrars.[23] Abuse-harboring registrars

[18] New gTLD Program Explanatory Memorandum Mitigating Malicious Conduct, 12 November 2010, https://archive.icann.org/en/topics/new-gtlds/explanatory-memo-mitigating-malicious-conduct-12nov10-en.pdf

[19] Unspecific CZDS contract language makes zone data access approvals a dice roll, by The Security Skeptic, August 13, 2019, https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html

[20] Citation - [Add links to consituency submissions and GAC communiques]

[21] Citation - [Add links to CCT Review Report], and The Statistical Analysis of DNS Abuse in New gTLDs Final Report https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

[22] Correspondence from the Independent Compliance Working Party to Jamie Hedlund, February 27, 2018, https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf

[23] Letter from Hedlund to Roache, https://www.icann.org/uploads/compliance_notice/attachment/1113/hedlund-to-roache-15mar19.pdf

are not an anomaly. Spamhaus (among others) tracks the most abused registrars, and certain registrars have been repeatedly identified year after year.[24]

The 2013 RAA includes a Cross Field Validation requirement for domain registration address data.[i] Cross field validation is a common, automated validity check done worldwide on the internet (e.g., if the house number exists on the street, which exists in the city and province, and the postal code is correct). This cross-field validation requirement was to become effective 6 months after ICANN and a working group of registrar volunteers "agreed that cross-field validation is technically and commercially feasible."[25] Six years later, ICANN has not required the implementation of this validity check, whcih has the potential to significantly reduce fraudulent domain name registrations.

The 2013 RAA also includes a Specification on Privacy and Proxy Registrations that contains requirements for privacy and proxy service registrations offered through affiliates and resellers of registrars accredited under the 2013 RAA. Among other elements the accreditation program requirements are to include detailed frameworks for provider responses to requests from law enforcement authorities and intellectual property holders. [add stats on abuse in privacy/proxy providers] Six years later, ICANN has not implemented these requirements.

ICANN has asserted that it lacks enforcement mechanisms to contend with systemic abuse. As stated by the head of ICANN Compliance, Jamie Hedlund, in an April 2018 correspondence: "There are potential limitations on the actions that ICANN org can take in addressing DNS infrastructure abuse. Neither the Registry Agreement (RA) nor the 2013 Registrar Accreditation Agreement (RAA) has enforceable provisions prohibiting or authorizing sanctions against systemic DNS infrastructure abuse. In addition, the RA and ICANN policies as currently defined do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names. Similarly, the RAA does not authorize ICANN org to require registrars to suspend or delete potentially abusive domain names."[26] However, ICANN Compliance has not publicly requested specific changes to the RAA or RA, nor has it incorporated functionality to monitor service levels, penalties, or circumstances that warrant suspension of a registrar's or registry's privilege to process new registrations. Further, Compliance also has failed at a minimum level, to leverage the work of reputable security experts in the community and implement measures to address abuse flagged by them.

gTLD Registry Agreements - Law enforcement, governments, security communities, and commercial and user interests groups all argued for contractual obligations to mitigate abuse during the deliberations of the new gTLD base registry agreement (RA), the update of this agreement, and implementation of these agreements, including Spec 11 of the RA. Few abuse mitigation measures emerged from the closed negotiations between ICANN Org staff and registries, and contracts do not include language or terms specifically addressing systemic

[24] The Spamhaus Project, spamhaus.org, https://www.spamhaus.org/statistics/registrars/

[25] https://www.icann.org/news/announcement-2014-02-07-en

[26] https://www.icann.org/en/system/files/correspondence/hedlund-to-vayra-04apr18-en.pdf

abuse and obligations of registries in this regard. From reports, it is evident that some accredited registries established practices to quickly and substantially increase domain registrations, many of which are used for abuse and criminal activities. ICANN Compliance failed to address this ongoing, systemic abuse.[27] Spamhaus (among others) tracks the most abused TLDs registries manage, and certain registries have been repeatedly identified year after year.[28]

Data and Advice from inside ICANN:

1. ICANN's own Security Stability and Advisory Committee has repeatedly published reports[29] documenting issues with the registration process. Recommendations have repeatedly urged registrars to improve WHOIS data validation, eliminate excessive WHOIS rate limiting, reconsider wholesale redaction of WHOIS point of contact data, and to act when notified of domain abuse. Such recommendations have largely been ignored or deferred. In 2012, for example, an SSAC recommendation that registrars adopt multi-factor authentication was largely ignored. It leads one to consider if the flurry of hijackings[30] of government and private domain accounts in 2019 could have been mitigated if registrars had heeded SSAC's advice or if ICANN had made multifactor authentication a contractual obligation. ICANN also failed to act on additional SSAC recommendations aimed at registries that would help improve DNS security, stability and resiliency. [add additional]

2. [Additional information & cits to be added] Recommendations from the Government Advisory Committee, e.g., safeguards applicable to all new gTLDs[cite] also call for WHOIS validation, security checks, security threat reporting and complaint handling. [add additional key communique SSR recommendations and Constituency filings]

3. Similar recommendations offered by review teams commissioned by ICANN to assess WHOIS[31] and Competition, Consumer Trust and Consumer Choice[32] have not been adopted by the ICANN Board. As of now, these have not been addressed in registry or registrar agreements with appropriate enforcement mechanisms. ICANN's Compliance Performance Measurements Reports[33] illustrate the gravity and longevity of the WHOIS inaccuracy problem, but the measurements are otherwise unhelpful. Compliance doesn't report details of resolution, and there is no transparency in the disposition process that ICANN and contracted parties employ,

---

[27] Correspondence from the Independent Compliance Working Party to Jamie Hedlund, February 27, 2018, https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf

[28] The Spamhaus Project, Spamhaus.org, https://www.spamhaus.org/statistics/tlds/

[29] https://www.icann.org/groups/ssac/documents

[30] https://arstechnica.com/information-technology/2019/01/multiple-us-gov-domains-hit-in-serious-dns-hijacking-wave-dhs-warns/

[31] https://www.icann.org/public-comments/rds-whois2-review-2018-09-04-en

[32] https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf

[33] https://features.icann.org/compliance/dashboard/report-list

and responses provided to complainant lack detail. [add additional text re review recommendations]

4. ICANN has one of the most definitive abuse reporting systems in the Domain Abuse Activity Report (DAAR) Program,[34] but has failed to respond to repeated requests to publish impactful reports that associate security threats to registrars and registries, despite having had the methodology and back-end service reviewed by external experts.[35] Neither the DAAR project nor the Specification 11 3b implementation provide sufficient information to satisfy the stated objectives of these activities, and arguably the most important objective is to allow for informed decision making by ICANN's community and the public. No registrar reporting is provided, in part, because rate limiting impedes the DAAR project. Many of the important measurements – for example, cumulative security threat counts over 365 days – are not published. In relation to engendering confidence in the new TLD program in this regard, ICANN falls short given its decisions to not published reports that provide visibility into abuse trends by TLD.

Identifying registries and registrars would give the ICANN community visibility into abuse that it does not currently have, data that would unquestionably facilitate informed policy making, and additionally add a measure of transparency and accountability to the domain name registration system that does not exist today.

ICANN Compliance

ICANN Org historically has stated in compliance and SSR2-related matters that it does not have the contractual tools necessary to enforce against registries and registrars. However, ICANN Org has never stated what tools it needs and how its current, narrow interpretation of the RAA and RAs hamper its work. While this has been a subject of community concern for over a decade, particularly during the negotiations over the 2013 RAA [cite], the closed-door negotiations between ICANN Org and contracted parties have not brought about the stronger contractual language necessary to aid enforcement.

ICANN Org has been unable to address abuse mitigation effectively under the existing Compliance regime, notwithstanding the abuse detection and mitigation obligations that ICANN's contracts with registries and registrars place on them. Contracted parties have been unable to find a consensus process to adopt or implement AGB obligations or recommendations from the GAC or the SSAC (e.g., SAC 101). The GAC advice concerning Specification 11 of the 2013 Registry Agreement, for example, emphasized three key provisions:

> 1. Registry-Registrar provisions to prohibit domains being misused for criminal activity and suspend as appropriate given applicable laws;

[34] https://www.icann.org/octo-ssr/daar

[35] https://www.icann.org/news/announcement-2018-07-20-en

2. Registry operators to perform technical analysis of their gTLD space to protect domains from pharming, phishing, malware, and botnets; and
3. Registries to maintain records of analysis, actions taken from them and also provide them to ICANN upon request.

Accredited parties do not consistently implement consensus policies and resulting contracts regarding abuse. Compliance has few options to enforce the agreements and has not exercised those enforcement clauses that do exist, taking into account the community's interpretation of the contract clauses on available avenues for enforcement. Leveraging contracts between ICANN and registrars and registries is important, in that it demonstrates public commitment to desired outcomes and gives ICANN Compliance the opportunity to enforce provisions on behalf of the community's interests. ICANN Org historically has had a relatively "hands-off" approach to these contracts -- for example, it has been more than six years since the Registrar Accreditation Agreement was reviewed and renegotiated, while ICANN Compliance states that they do not have the contractual tools necessary to enforce contractual issues with registries and registrars, which delays the development and establishment of an effective ICANN enforcement mechanism.

Known problems with bad actors "hiding out" in certain TLDs continue to frustrate efforts to eliminate security threats from the DNS. ICANN Org does not have a history of action or transparency in addressing this in specific TLDs. Transparent reporting of this behavior would help focus ICANN Org's and the community's effort toward eradicating DNS security problems and help re-establish trust for that portion of the namespace.

Further, ICANN's complaints process is confusing and lacks insightful or impactful data about abuse handling. [add text, and notes from RDS Review]

RECOMMENDATIONS:

1) Compliance - The Board and ICANN Org should fundamentally change the Compliance regime by taking the necessary steps to amend the RAA and RAs, establish procedures to address systemic abuse involving contracted parties, and move its registrar and registry compliance activites to an independent Compliance Office outsourced to an established auditing firm.

- Such changes must include amendments to the RAA and RAs that make specific abuse mitigation measures an explicit obligation. These amendments must provide Compliance with enforcement mechanisms that treat persistent, repeated violation of abuse agreements as seriously as failure to pay fees. Contract changes should be accompanied by an establishment of procedures to address systemic abuse in registrars and registries, including: act now using current abuse definition; have SSAC work with established abuse mitigation organizations to define "systemic abuse" for colloquial and legal use, and an acceptable level of abuse countermeasures per contracted party; amend contracts as soon as possible, the latest at next renewal, to include clauses on

systemic abuse and required abuse countermeasures, and make them enforceable and explicit. SLA agreements should be in place.

- As with other sectors that have inherent conflicts, such as financial institutions, ICANN needs to move its compliance activities to a neutral, third-party auditor. Since ICANN derives most of its funding from registrars and registries, it should separate its registrar and registry compliance activities to ensure neutral and effective compliance with contracts. ICANN should establish an independent Compliance Office outsourced to an established auditing firm, populated with staff with significant compliance experience and understanding of both DNS abuse mitigation and registrar and registry industries. The ICANN Board must empower the Compliance Office to react to complaints and require Compliance to initiate investigation and enforce against those aiding and abetting systemic abuse. This could include step by step authority for the escalation of enforcement measures and implementable actions that can be utilized for failure to remedy within specified timeframes. Compliance should partner with complainants and serve the public interest. Compliance's default approach should involve SLAs on enforcement and reporting, clear and efficient, processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure. [add RDS Review recommendations] If any complaint is found to be specious, the public record should reflect that. Compliance's history of keeping complainants and the public in the dark and accommodating contracted parties rather than the public interest must end.

2) Abuse Definitions & Reporting - ICANN Board and ICANN Org should overhaul ICANN's approach to DNS abuse definitions, tracking and reporting, including implementing community review recommendations and other security-related actions, act now using the current "DNS abuse" definition and in parallel use international conventions to evolve the definition, create a single portal for all complaints, and make public reporting mandatory.

- Implement the CCT Review and RDS (WHOIS) Review recommendations,[36] and other security-related actions based on current, community vetted abuse definitions, without delay, but no later than 2020.
- Use the current DNS Abuse definition and take into account the processes and definitions outlined in the Convention on Cybercrime.[37]. Forego new efforts to have ICANN Org or the ICANN community re-define DNS Abuse and instead adopt the additional term and evolving external definition of "security threat"—a term used by the ICANN DAAR project, the GAC (in its Beijing Communique and for Spec 11), and operational security communities – to use in conjunction with ICANN DNS Abuse definition. Further, ICANN should use The Convention on Cybercrime[38] as a reference resource for identifying universally acceptable agreement on the definition of

[36] See DNS Security Abuse contained in the CCT Review (footnote 11), which reflected definitions proposed in the Revised New gTLD Program Safeguards Against DNS Abuse dated July 2016.
[37] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[38] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

general types of cybercrimes and related security threats. Employing this threat taxonomy developed by experts, in addition to its current DNS Abuse definition, will enable ICANN to better address the global security and stability threats outlined above and the evolving threat landscape. ICANN should use these resources to align its policies with the Treaty and to minimize ambiguous language in its contracts with contracted parties and implementation plans.

- ICANN should establish and maintain a single complaint portal for all complaints, that ~~which~~ automatically directs reports to relevant parties. The system would purely act as inflow, with only summary and metadata flowing upstream. It should be mandatory for all gTLDs; ccTLDs should be invited to join. ICANN should publish yearly reports, using the data created by the system. The process would work as follows: 1) Complaint submitted, ticket number created, sent to registrar; 2) Registrar responds, ticket closed. Registrar does not, goes to registry; and 3) Registry responds, ticket closed. Registry does not respond, it goes to ICANN. Reports to non-participating ccTLDs to be forwarded via email. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). The portal also should enable improved complaint reporting and security threat reporting. Public reporting of all complaints to all contracted parties -- Registry, Registrars, Privacy/Proxy Providers (upcoming) -- and related data, should be mandatory. In addition, to ensure DAAR's utility, we recommend: data gathering for DAAR should not be rate-limited; published reports should identify the registries and registrars that most contribute to abuse, and should illustrate entities with persistently very high abuse domain registrations; published reports should provide tabular data in an accessible, processible form, in addition to the visual (graphical) data; and the DAAR project should have access to pricing data.

3) Policies and agreements with Contracted Parties – adopt new ones that meaningfully impact mitigation of DNS abuse and security threats, including changes to WHOIS, incentives for contracted parties for abuse mitigation, incorporate measures to mitigate "DNS abuse" and "security threats" in agreements with contracted parties, estalish a performance metrics framework, and institutionalize training and certifications for contracted parties and key stakeholders.

- Update key policies and practices impacting security threat mitigation. Changes to WHOIS policy have created serious impediments for security investigators and threaten DNS security, stability and resiliency. These have been documented through industry surveys, data analyses and numerous stakeholder input. No uniform method of access to non-public WHOIS data is defined, even for law enforcement. As a matter of urgency, ICANN should ensure access for parties with legitimate purposes via contractual obligations and with rigorous compliance, rather than as a voluntary implementation. An ETA must be published within 6 months of this report's publication. WHOIS rate limiting practices by contracted parties are impediments to security threat mitigation

and should be prohibited for ICANN Compliance and Security, for entities related to the DAAR project and for other reporting systems like DAAR, for security threat investigations, and for law enforcement. Establish and rigorously enforce uniform Centralized Zone Data Service requirements to ensure continuous access for these purposes. ICANN org must enforce norms within XXX.

- Incentivize contracted parties to mitigate abuse and security threats. Historically, ICANN.org has rewarded contracted parties with fee reductions to incentivize certain business practices (e.g. domain tasting). The existing contract framework enables ICANN to impose such changes unilaterally and immediately. ICANN Org should take the following actions: 1) That contracted parties with portfolios that have less than 1% abusive domain names, as identified by commercial providers and/or DAAR, receive a fee reduction. This could be a reduction from current fees, or ICANN could increase the current per domain name transaction fee, and provide a Registrar with a discount down to the current $0.18 per domain name for low abuse levels. 2) That Registrars receive a fee reduction for each domain name registered to a verified registrant. 3) That any RSTEP fees be waived when in connection with RSEP filings that will demonstrably mitigate DNS abuse, and that any Registry RSEP receives preapproval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant. Currently, Registry Operators who submit an RSEP that is deemed by ICANN Org to raise potential security and stability concerns are subjected to an RSTEP panel and associated fees up to $100,000—effectively a tax on innovation. Waiving such fees could promote, instead of impede, innovation focused on minimizing DNS abuse.

- Incorporate measures to mitigate "DNS abuse" and "security threats" in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, as necessary and essential contract obligations. This should include, as a priority, provisions that establish thresholds of abuse (3% of registration or 30 total whichever is the higher) at which compliance inquiries are automatically triggered, with a higher threshold (10% of all registrations) at which registrars and registries are presumed to be in default of their agreements. This approach also was underscored in the CCT Review (citation) and SSR2 recommends it. In addition, ICANN should: publish a list of "enforcement tools" identified by ICANN Compliance as needed to combat abuse and security threats; coordinate closely with relevant non-contracted parties to identify additional gaps within ICANN's contracts that contribute to abuse and security threat activities; develop a list of impactful contractual updates to guide negotiations; ensure non-contracted party representatives who are thought leaders on abuse and security threat mitigation are involved in all base contract negotiations and endorse changes.

- ICANN's legal authority to address compliance, security and/or stability of the DNS, is based on the bylaws and in relation to compliance by Registrars the Service Level Agreements. During the review, it became apparent that the scope to mandate compliance by Registrars is limited to the provisions of the SLAs and therefore it is recommended that ICANN: establish a performance metrics framework to guide the level of compliance by Registrars for not only WHOIS inaccuracy but other elements that

affect abuse, security and resilience; allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics; amend the SLA renewal clause from 'automatically renewed' to a cyclical 4 year renewal with a review clause included. This review period would consider level of compliance to the performance metrics by the Registrar and inclusion of requirements to strengthen the security and resilience, where during the contract period non-compliance was evident.

- Institutionalize training and certifications for contracted parties and key stakeholders -- Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers -- in areas identified by DAAR and other sources on common methods of abuse, and mitigation efforts. Features should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Pure inflow system, with metadata flowing upstream; Quarterly/Yearly public reports on complaints, actions, etc. and analysis; Evidence sharing not required, just summary information is reported, e.g. registrar response, reasoning (spurious, appropriate evidence, internal investigation, time stamps).

[i] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy Except as provided in Section 3 below, within fifteen (15) calendar days after receiving any changes to contact information in Whois or the corresponding customer account contact information related to any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar will validate and, to the extent required by Section 1, verify the changed fields in the manner specified in Section 1 above. If Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.