With regard to the ICANN org blog:https://www.icann.org/news/blog/icann-org-s-multifaceted-response-to-dns-abuse

1. The blog says: " the domain names and the data collected by the system will be shared with parties who are in a position to take action, such as registrars and registries, and in some cases with national and international law enforcement organizations."
    a. What specific actions is ICANN expecting registries and registrars to take?

       By leveraging the Registrar Stakeholder Group's Guide to Registrar Abuse Reporting Practices, ICANN org is reporting domains identified by the system to represent a subset of security threats (specifically, phishing or malware distribution). ICANN org would expect registrars, and where applicable, registries, to investigate the report(s) and respond appropriately.

    b. For example, is ICANN encouraging suspension of name resolution or of the registration, or the registrant account?

       ICANN org is not encouraging any specific course of action in response to the reports. As stated above, ICANN org would expect registrars, and where applicable, registries, to investigate the report(s) and respond appropriately.

    c. Will ICANN ask registrars and registries to report on the efficacy of these actions? If so, when and on what cadence?

       ICANN org is not asking registrars and registries to report on the actions taken or the efficacy of any actions taken. There is nothing requiring such reporting under the ICANN agreements. However, the identified domains and actions taken in response to ICANN org's reports may be included in registries' statistical reporting referenced in Specification 11 3(b). Also, if a domain that has been reported as part of this project continues to resolve and remains a security threat, ICANN org may enquire about the actions taken.

    d. ICANN should publicly report per registrar & registry action:
        i. How many names has it identified as suspicious/malicious?
        ii. What's the number of domain names that each registry/registrar has taken action against? And what action was taken
        iii. When can we expect ICANN public reporting and on what cadence?

       Thank you for the suggestions. ICANN org has no current plans to issue reports on a particular cadence.

2. What distinguishes ICANN's participation in the face of the pandemic from how they've participated in the past?

Assuming this question is in reference to the actions of ICANN Compliance, in response to the current pandemic ICANN Compliance is screening complaints for those related to COVID-19 pandemic-related terms and processing these complaints with high priority.

a. The blog says: "ICANN Compliance uses data collected in audits (described in more detail below) to assess whether registries and registrars are adhering to their DNS security threat obligations." What will Compliance do that it has not done until now?

Beginning with the most recent registry audit, ICANN Compliance has implemented a risk-based approach to focusing the audit requests for information and compiling the data from responses. Rather than audit for compliance with the entire contractual agreement, ICANN Compliance focused its recent registry audit on compliance with applicable DNS abuse obligations. The Audit Program will follow this same approach when it launches the registrar audit later this year.

b. Is Compliance making audit data associated with US-based registrars available to States Attorney Generals and the US Attorney General?

As with all audit reports, the Report on the Registry Operator Audit for Addressing DNS Security Threats is published on icann.org and available publicly. The link to the document can be found here https://www.icann.org/news/announcement-2019-09-17-en. ICANN Compliance does not publish or share data collected from contracted parties during an audit, as this information is submitted to ICANN org confidentially.

3. The blog states (the obvious) that ICANN isn't a regulator of Internet content, but it doesn't address ICANN's public interest remit. Multiple entities have asked ICANN to better govern the manner in which domain names are registered, and now especially, everyone is asking ICANN to hold contracted parties to greater accountability to prevent domains from being registered by malicious actors, especially for pandemic-related fraud and abuse. This requires greater scrutiny during the registration process. What actions are ICANN taking that address this?

The Registrar Accreditation Agreement does not specify a mechanism by which "greater scrutiny" can be applied during the registration process, nor is ICANN org able to ascertain who a "malicious actor" would be prior to their use of the domain for malicious purposes.

ICANN org has, as described in the referenced blog and in response to these questions, initiated a project to identify COVID-19-related domain name abuse and report that abuse to those who can take action to mitigate the abuse, namely registrars, registries, and in some cases, international and national law enforcement.

a. In addition to high volumes of fraudulent domain names containing pandemic-related strings with which criminals try to fool Internet users, random looking or otherwise auto-generated names that are easy to register in volume and are being used by the hundreds to perpetuate pandemic-related phishing attacks. What actions are ICANN taking that addresses this?

As described in another recent ICANN org blog, ICANN org is using a set of terms to identify domains that appear to be leveraging the COVID-19 pandemic. Those names are then compared to information collected by a set of reputation providers to identify if they are being actively used for phishing or malware distribution attacks. When the reputation provider data suggests a domain may be used for phishing or malware distribution, ICANN org collects information related to that domain as specified in the Registrar Stakeholder Group's Guide to Registrar Abuse Reporting Practices. ICANN org then provides that information to the registrar, as well as potentially to the registry and international and national law enforcement. As stated above, ICANN org would expect registrars, and where applicable, registries or the other entities, to investigate the report(s) and respond appropriately.

Additionally, ICANN org is unaware of systemic use of auto-generated names for COVID-19-related phishing or malware distribution attacks. If members of the SSR2 Review Team are aware of any information related to systemic use of auto-generated names as mentioned, we encourage them to provide that information to the OCTO team (octo@icann.org) so that we can investigate how we might include that information in our COVID-19-related DNS abuse project.

b. Recommended actions contained in SSR2's draft report could help mitigate pandemic-related domain name abuse. Is the ICANN Board and staff reconsidering any of these actions?

As the recommendations found within the SSR2 draft report have not yet been approved by the Community or Board, ICANN org has not considered them for mitigation of pandemic-related domain name abuse. ICANN is always open to hearing feedback from the community and looks forward to receiving the finalized recommendations from SSR2.

c. Recommendations from others over the last few years also would help mitigate pandemic-related domain name abuse – especially the substantially increased phishing attacks that harm users. Is the ICANN Board and staff reconsidering any of these actions? Including:

i. will ICANN move to ensure domain name registrant data is validated? Or at least implement cross-field validation?

ICANN org enforces existing registration data validation requirements via the Whois Accuracy Program Specification of the 2013 Registrar Accreditation Agreement (RAA). This requires registrars to validate certain registration data fields, including email addresses, telephone numbers and postal addresses. See more information here: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy.

Regarding Across Field Validation, ICANN org notes that it is not in ICANN org's remit to unilaterally "implement cross-field validation" and the requirement is not yet effective per Section 6 of the Transition Addendum to the Registrar Accreditation Agreement. ICANN org notes that as of late 2019, despite significant efforts by ICANN org and registrars, there has not been mutual agreement on identification of a commercially and technically feasible solution for the implementation of AFAV. ICANN org formally paused efforts to implement Across Field Validation for a period of two years. Following the pause, ICANN org will reassess the market for commercial solutions that may have advanced since the last assessment in late 2017.

Additionally, a report assessing the impacts of the EPDP Phase 1 recommendations on non-policy procedures, such as Across FIeld Validation, is expected to be issued by ICANN org later this month .

ii. will ICANN put in place an Acceptable Use Policy that applies specifically to parties that register large numbers of domains, that requires registrants to apply for (and be validated for) bulk registration services? Further, will ICANN put in place an obligation to distinguish domain names registered by legal entities from those registered by natural persons, classify parties that use bulk registration services as legal entities, and require unredacted access to the registration data of legal entities?

It is unclear what is meant by ICANN org putting in place an "Acceptable Use Policy", to whom such a policy would apply, or what is meant by "bulk registration services". With respect to requirements imposed on "parties that register large numbers of domains", it would appear this would raise a number of policy-related questions, e.g., what would entail "large" numbers of domains, over what timeframe would that be measured, what validation requirements would be needed for such registrations, etc. Additionally, there are ongoing discussions as part of the policy development process regarding the issue of distinguishing between the registrations of legal and natural persons. Therefore, it would appear to be premature for ICANN org to impose such obligations.

iii. will ICANN maintain and publish a current list of validated bulk registrants (who are from above defined as not natural persons)?

As noted above, “validated bulk registrants” is undefined. Therefore, this request would appear to be premature.

iv. will ICANN disallow registration transactions that involve large numbers of random-looking algorithmic domain names?

ICANN org cannot unilaterally impose contractual obligations. As such, it is unclear how ICANN org would be able to disallow registration transactions of any kind, much less transactions for a particular class of domain names.

v. will ICANN disallow, for a period of one year, the re-registration of any bulk-registered domain name that has been used in a criminal cyberattack?

As noted above, it is unclear how ICANN org would be able to impose such a restriction.