Before the
U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
Washington, D.C. 20528

In the Matter of	)	
	)	
Cyber Incident Reporting for Critical	)	Docket No. CISA-2022-0010
Infrastructure Act (CIRCIA) Reporting	)	
Requirements	)	

COMMENTS OF INTERNET INFRASTRUCTURE COALITION

Christian Dawson, Executive Director
Ann Morton, Senior Policy Director
Internet Infrastructure Coalition
2920 W. Broad Street, Suite 80
Richmond, VA 23230
dawson@i2coalition.com
ann@i2coalition.com

July 3, 2024

COMMENTS OF INTERNET INFRASTRUCTURE COALITION

EXECUTIVE SUMMARY

The Internet Infrastructure Coalition ("i2Coalition") presents the following core arguments in its CIRCIA NPRM comments:

- **Multistakeholder Internet Governance Should Direct the DNS Exception Implementation.** The U.S. government was the primary architect of the multistakeholder system of Internet governance. The principles it helped to create, which it has repeatedly renewed its commitments to, should serve as the framework for shaping the DNS Exception. By aligning with the principles of multistakeholder governance that the U.S. government has fostered globally, the DNS Exception can contribute to a more secure, stable, and resilient global Internet ecosystem that benefits Internet users worldwide. This requires CISA to make decisions in this rulemaking that properly account for ICANN's role, promote global cooperation, preserve innovation and flexibility, and emphasize the need for transparency and accountability on a global scale for global infrastructure.

- **A Global DNS Reporting Process Can Be Created Within the ICANN Framework.** Cyber incident reporting for the specific DNS services and technical functions under ICANN governance requires a distinct approach. Developing a global reporting ecosystem within the ICANN framework, using CISA's approach as a starting point, would be more effective than a fragmented patchwork of regional reporting regimes. CISA should actively prioritize global harmonization efforts, and work with organizations like the i2Coalition to catalyze stakeholder conversations and use ICANN as the ideal venue for this work at the DNS level. This approach would ensure that DNS cyber incident reporting – in pursuit of improving the security and stability of the Internet's global infrastructure – is managed globally, enhancing the safety and resilience of the Internet for all users.

- **CISA Should Apply the DNS Exception Criteria Coherently and Consistently.** As CISA refines its approach to the DNS Exception, it must follow a consistent basis for applying the exception criteria. Including domain registries and registrars in the exception fully aligns with established governance principles and enhances the coherence of the exception framework. This approach promotes the goals of fairness, consistency, and effectiveness in managing cybersecurity risks within the global DNS ecosystem. Fundamentally, DNS registry and registrar functions fall within the scope of the statutory DNS Exception: they are clearly governed by ICANN, and therefore qualify to be exempt from reporting under CIRCIA.

I. INTRODUCTION AND STATEMENT OF INTEREST

The Internet Infrastructure Coalition ("i2Coalition") respectfully submits comments regarding the Department of Homeland Security's Proposed Rule in the above-referenced docket outlining requirements for defined covered entities within the United States to implement cyber incident reporting, among other obligations (the "Proposed Rule"), as set forth in the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA").[1]

The i2Coalition is a global organization that supports and represents the companies that build, maintain, and operate the Internet's infrastructure. Members include cloud providers, data centers, web-hosting companies, and domain registries and registrars. Our members, mostly small- to medium-sized businesses who operate globally, create a fundamental layer upon which user-facing Internet applications, services, and platforms rely and enhance that layer for interoperability and security.

The role of the i2Coalition's domain registry and registrar members in Internet infrastructure operations is particularly notable for this proceeding. Our domain registry and registrar member companies provide vital technical services and functions that are governed by the Internet Corporation for Assigned Names and Numbers (ICANN), the not-for-profit entity responsible for the technical coordination of the Internet's domain name system (DNS).

The U.S. Department of Commerce established ICANN as a result of President Clinton's 1997 Framework for Global Electronic Commerce, which directed the Department of Commerce to privatize the management of the Domain Name System (DNS). The goal was to increase international participation in the Internet and make it a new medium for commercial exchange. Promoting a secure global Internet ecosystem and the responsible use of its enabling infrastructure have become core goals of i2Coalition and its members, and we work closely on these objectives with stakeholder communities at ICANN. We appreciate the Department's publication of the Proposed Rule and the invitation to provide these comments.

---

[1] *See Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*, Proposed Rule, 89 FR 23644 (Apr. 4, 2024).

Our comments focus on the DNS Exception, and the related policy and legal questions that CISA has presented in the rulemaking text that are unique to the DNS community. Most fundamentally, we submit that DNS registry and registrar functions are clearly governed by ICANN, and should, therefore, be exempted from reporting under CIRCIA because they are in the scope of the statutory DNS Exception.

II. DNS EXCEPTION: RESPONSES TO AREAS OF INQUIRY

Our responses below to the specific areas of inquiry posed in the rulemaking text detail both technical and policy reasons why CISA should make clear in the final CIRCIA rules that domain registrars and registries clearly fall within the scope of the DNS Exception.

Para. 42: The covered entities which CISA proposes this exception apply to, including whether any additional covered entities involved in DNS operations, such as domain name registries and registrars, should be considered by CISA for this reporting exception. If so, how do those covered entities, or specific functions thereof, meet the statutory requirements, including specifically how the entity or its functions may "constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority"?

Domain Name Registries and Registrars Clearly Fall Within the Scope of the CIRCIA DNS Exception. The i2Coalition proposes that CISA expand the implementation of the DNS reporting exception to explicitly include domain name registries and registrars. These entities perform essential functions within the Domain Name System (DNS) and are critical to the stability, security, and resilience of the Internet's infrastructure. This exception should apply specifically to the core DNS services provided by registries and registrars that are governed by their contractual, but also their practical requirements to abide by consensus policies developed through the ICANN policy process in order to provide their services within the DNS ecosystem. The exemption would only apply to those core DNS services and not to the entire company or any other services the company might offer.

Domain name registries and registrars are integral to the broader ecosystem of the Internet's infrastructure. The DNS itself is recognized as a component of critical infrastructure under CISA's

Information Technology Sector-Specific Plan[2]. While not every service provided by registries and registrars may individually qualify as critical infrastructure, the collective ecosystem managed under ICANN's governance framework does. This governance ensures that the policies and operations concerning the DNS are subject to rigorous, multi-stakeholder processes, which promote the overall security, stability, and resiliency (SSR) of the DNS.

The governance by ICANN and the Internet Assigned Numbers Authority (IANA) ensures that these core services are subject to comprehensive multi-stakeholder policies. ICANN's policies, developed through a collaborative, consensus-based process involving diverse global stakeholders, cover a range of issues vital to the SSR of the DNS. These policies align with the statutory requirements included in CIRCIA, ensuring that domain registries and registrars operate under a framework that promotes transparency, accountability, and security.

It is important to distinguish between the services and functions provided by a company and the company itself. The core DNS functions performed by registries and registrars under ICANN governance should be exempt from CIRCIA reporting requirements, recognizing their critical role within the broader ecosystem of Internet infrastructure. This does not extend to other services that these companies might offer outside of their ICANN-governed DNS operations. For example, while a registrar may offer web hosting or other IT services, only its DNS registration services, managed under ICANN policies, should be considered for the DNS Exception.

ICANN's bylaws[3] explicitly mandate the organization to ensure the SSR of the global DNS, encompassing measures for cyber incident reporting and response. This governance framework includes the policies and security measures implemented by registries and registrars, which align with the goals of

[2]Information Technology Sector-Specific Plan An Annex to the NIPP 2013
https://www.cisa.gov/sites/default/files/2023-01/nipp-ssp-information-technology-2016-508%20%281%29.pdf
[3] Bylaws for Internet Corpoation for Assigned Names and Numbers
https://www.icann.org/resources/pages/bylaws-2012-02-25-en

CIRCIA. Therefore, the cyber reporting obligations should fall under ICANN's purview, allowing for a consistent, global approach rather than a fragmented, jurisdiction-specific one.

Para. 43: Information, facts, or other views that describe or explain the relationship between ICANN and domain name registries and registrars, as well as specific cyber incident and ransom payment information that must be reported to ICANN by entities accredited by ICANN.

Rationale for Expansion of DNS Reporting Exception Based on ICANN Relationship. The governance framework of ICANN overseeing domain name registries and registrars is crucial to the functioning of the Internet's DNS. ICANN is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. Domain name registries and registrars are entities accredited by ICANN to manage and distribute domain names within specific generic top-level domains (gTLDs), such as .com, .org, .net, etc.

Domain registries are responsible for managing top-level domains (TLDs) at the highest level of the DNS hierarchy. They maintain the authoritative databases for their respective TLDs and coordinate with ICANN to ensure the stability and security of the DNS. Registrars, on the other hand, are entities authorized by registries to register domain names to individuals and organizations. They act as intermediaries between domain registrants and registries, facilitating the registration, renewal, and transfer of domain names.

ICANN has established a governance framework to oversee domain registries and registrars, outlining their rights and responsibilities in managing domain names. ICANN’s system encompasses the agreements that registries and registrars have entered into with ICANN, which include provisions addressing DNS security and incident reporting. Specifically, ICANN's Registrar Accreditation

Agreement (RAA)[4] and Registry Agreement (RA)[5] outline the obligations of accredited entities regarding cybersecurity incident reporting.

Under these agreements (section 4.1 in the RAA, section 2.2 in the RA), accredited entities are required to comply with consensus policies of ICANN. The RAA has a further obligation under section 3.20 to report specific cyber incidents to ICANN, with a breakdown of general reporting responsibilities within the RA detailed within Specification 10, section 7.3. Incidents requiring a report to ICANN may include security breaches, data breaches, and other cybersecurity threats affecting domain names and associated services. The reporting requirements aim to enhance transparency, accountability, and coordination in addressing cybersecurity risks within the DNS ecosystem.

ICANN maintains multiple channels and mechanisms for accredited entities to either identify and measure or report cyber incidents promptly, including the measurement-focused DNS Security Threat Mitigation Program[6] and the Domain Name Security Threat Information Collection & Reporting (DNSTICR)[7], which is an outward-facing program through which ICANN reports to registries and registrars. These reporting mechanisms facilitate timely notification and response to security incidents, enabling ICANN to coordinate with relevant stakeholders to mitigate threats and safeguard the integrity of the DNS.

While current ICANN cybersecurity measurement and reporting obligations may not collectively be as robust or comprehensive a framework as is proposed by CISA, they do provide evidence that ICANN has cyber reporting within its scope as part of its SSR responsibilities. The baseline system ICANN has in place makes it simple for a more robust cybersecurity reporting framework to be

[4] Registrar Accreditation Agreement (RAA) – Approved 21 January 2024
https://www.icann.org/resources/pages/registrars/registrars-en
[5] Base Registry Agreement - Approved 21 January 2024
https://www.icann.org/en/registry-agreements/base-agreement
[6] DNS Security Threat Mitigation Program
https://www.icann.org/resources/pages/dns-security-threat-mitigation-2021-07-19-en
[7] Domain Name Security Threat Information Collection & Reporting (DNSTICR)
https://www.icann.org/dnsticr-en

developed through the multistakeholder process. Moreover, it provides a foundation for a global method of cybersecurity reporting that would allow ICANN and its contracted parties to better maintain the security, stability, and resiliency of the Internet's domain name system, ensuring a safe and reliable online experience for users worldwide.

Para. 44: **What types of covered cyber incidents could be unique to, or have a unique impact on, the covered entities that would be exempt from reporting under CIRCIA based on the scoping of the proposed DNS exception?**

The proposed implementation of the DNS Exception, which should include domain name registries and registrars, involves entities that operate critical components of the Internet's infrastructure and manage its addressing system. The impact of cybersecurity incidents on the DNS can be profound, given the essential role of the work done by domain name registries and registrars, but this impact is distinctly global. It is vital to understand this distinction, which is exactly why the overall security, stability, and resilience (SSR) of the DNS is under ICANN's governance. Because the impact of DNS-related cyber incidents is global, it would be untenable and unscalable to utilize a model in which each jurisdiction on the globe could seek its own DNS cyber reporting regime using its own methods and requirements.

Instead, with the DNS Exception in place, the ongoing development of DNS registry and registrar reporting frameworks within the ICANN multi-stakeholder community will further enhance the resilience and trustworthiness of the DNS ecosystem, which is constantly under SSR review as part of standard ICANN processes[8]. This work is fundamental to, and mandated by, ICANN's bylaws.

[8] ICANN Security, Stability, and Resiliency Review (SSR)
https://www.icann.org/resources/reviews/specific-reviews/ssr

Para. 45: What are the potential consequences of covered cyber incidents that would not be reported to CISA based on the proposed DNS exception (e.g., impacts to the functionality of the internet or to services offered to critical infrastructure)?

Proper scoping of the DNS Exception would exempt domain registries and registrars from CIRCIA's reporting requirements, thereby streamlining processes and reducing regulatory burdens for these entities. Nonetheless, the potential consequences of cyber incidents that would not be reported to CISA must be considered. These incidents can significantly impact the functionality of the Internet and services offered to critical infrastructure, underscoring the need for a global, rather than regional, reporting system.

Impacts on the Internet's Functionality. Cyber incidents exploiting the DNS infrastructure can have far-reaching consequences for the Internet's functionality. For example, DNS hijacking can redirect users to malicious websites, leading to widespread phishing attacks and malware distribution. Such disruptions not only affect individual users but also undermine trust in the Internet's reliability. A global reporting system, coordinated through ICANN's multi-stakeholder model, would enhance the ability to detect and mitigate these incidents more effectively, ensuring a more resilient Internet.

Impacts on Services Offered to Critical Infrastructure. Critical infrastructure sectors rely on the stability and security of the DNS. Unreported cyber incidents can disrupt the operations of these sectors, including healthcare, finance, transportation, and energy. A global reporting system would enable international sharing of threat intelligence and best practices, enhancing the protection of critical infrastructure worldwide.

Erosion of Trust and Operational Disruptions. Frequent or severe cyber incidents that go unreported can lead to a perception of unreliability in the Internet's infrastructure. Users and businesses may experience intermittent access issues, slow response times, or difficulty in resolving domain names. This erosion of trust can have broader economic impacts, including financial losses for businesses and increased costs for incident response. By promoting a global system of reporting, the entire Internet

community can ensure the continued stability, security, and trustworthiness of the Internet, benefiting users and critical infrastructure providers worldwide.

Para 46: What are the specific technical functions that DNS entities perform or provide in order to support the DNS versus related, but separate commercial offerings? How would this apply to different DNS entities such as root server operators, domain name registries, and domain name registrars?

Rationale for Expansion of DNS Reporting Exception Based on Technical Functions. DNS entities perform specific technical functions to operate and support the integrity of the DNS, which are distinct from related commercial service offerings they may provide. It is helpful to break down these functions and how they apply to different DNS entities such as root server operators, domain name registries, and domain name registrars:

1. **Root Server Operators (already exempted under Proposed Rule)**
    - **Function:** Root server operators maintain and operate the root name servers, which are a crucial part of the DNS hierarchy. These servers store the authoritative list of TLD name servers and their IP addresses.
    - **Role:** Root server operators ensure the availability and responsiveness of the root name servers, facilitating the resolution of DNS queries from recursive resolvers to the appropriate TLD name servers.
2. **Domain Name Registries**
    - **Function:** Domain name registries manage and maintain the authoritative databases for specific TLDs. They are responsible for accepting and processing domain name registrations, as well as managing domain name records and associated information.
    - **Role:** Registries maintain the integrity and consistency of the DNS database for their respective TLDs, ensuring that domain names are registered and managed accurately and securely. They also implement policies and procedures to prevent DNS abuse and maintain the stability of the TLD.

3. **Domain Name Registrars**
    - **Function:** Domain name registrars are entities authorized to register domain names for individuals and organizations. They provide domain registration services to customers, facilitating the process of acquiring and managing domain names.
    - **Role:** Registrars act as intermediaries between domain registrants and registries, processing domain registration requests, renewals, and transfers on behalf of customers. They also provide additional services such as web hosting, email hosting, and website building tools, for which they are not seeking exemption.

While these DNS entities may offer related commercial services, such as web hosting, email services, or website development, it is essential to differentiate those offerings from the core technical functions that the DNS entities provide that support the DNS and involve the management, operation, and maintenance of critical DNS infrastructure and databases, ensuring the smooth, reliable and seamless resolution of domain names to IP addresses across the Internet. Accordingly, because root server operators, domain name registries, and domain name registrars all play distinct roles in supporting the DNS through their specific technical functions, all three should be exempted from CIRCIA reports under the DNS Exception.

Para. 47: What cyber incident reporting requirements, either in the United States or internationally, are DNS entities currently subject to? To what government agency or other entity must those entities report cyber incidents? Please describe the specific cyber incident reporting requirement (e.g., timing and trigger requirements; details that must be reported; mechanism for reporting; supplemental reporting requirements).

Current Cyber Incident Reporting Requirements for DNS Entities. DNS entities, including domain registries and registrars, are subject to various cyber incident reporting requirements both in the United States and internationally. However, it is important to differentiate between the broad cybersecurity requirements imposed on companies and the specific requirements related to DNS services and functions. While companies in this sector face a range of reporting obligations, the specific DNS

services and functions we seek to exempt as within the scope of the DNS Exception fall into a distinct category that requires separate consideration.

Broad Reporting Requirements for Companies. In the United States, covered DNS entities must comply with reporting requirements set by the Department of Homeland Security (DHS). For instance, the DHS's Cybersecurity and Infrastructure Security Agency (CISA) requires the reporting of significant cyber incidents affecting critical infrastructure sectors through its Cyber Incident Reporting Portal. Internationally, the European Union's NIS Directive obligates DNS service providers to report significant incidents affecting service security to national cybersecurity authorities, usually within 24-72 hours. Additionally, the General Data Protection Regulation (GDPR) mandates reporting data breaches involving personal data to relevant data protection authorities within 72 hours. ICANN also imposes reporting requirements on DNS entities for DNS abuse and security incidents as part of their contractual obligations[9].

Specific Reporting Requirements for DNS Services. While these broad reporting requirements apply to companies, the specific DNS services that we seek to exempt involve different considerations. These services, which include domain registration and management functions, operate within a framework governed by ICANN. Within the ICANN RAA, in section 3.20, an accredited Registrar has a seven-day window through which to report a security breach, including a detailed description of the type of unauthorized access, how it occurred, the number of registrants affected, and any action taken by the Registrar in response. Registry reporting requirements, found in Specification 10, section 7.3, are more general, but have a shorter 24-hour reporting requirement.

Opportunity to Create a New Global Reporting System. Since the DNS technical functions operate and perform subject to a global ICANN governance framework, it is sensible for DNS cyber incidents to be reported under a global system that firmly rests within ICANN's purview. The DNS

[9] ICANN's Major Agreements and Related Reports https://www.icann.org/resources/pages/agreements-en

Exception presents an opportunity to develop an effective global reporting system. Cyber incidents affecting the DNS can have global impacts, which require coordinated, international responses.

A unified global reporting system, coordinated through ICANN, would offer significant benefits over a regional approach. It would ensure consistent reporting standards, facilitate international cooperation and threat intelligence information sharing, and enable the pooling of resources and expertise. This approach aligns with the inherently international nature of the Internet and the necessity for global coordination on security and stability. It promotes a more cohesive and robust response to cyber threats, especially those that could involve simultaneous, coordinated attacks on Internet infrastructure across multiple jurisdictions. It also avoids the imposition of a fragmented patchwork of potentially duplicative or conflicting regional reporting requirements on inherently global Internet infrastructure, enabling better coordination and quicker responses to mitigate threats.

There is an opportunity to utilize CISA's approach described in this rulemaking as a foundation for developing a global reporting ecosystem within the ICANN multi-stakeholder model. Such a system does not currently exist but is essential for the security and stability of the Internet. While ICANN would be unlikely to initiate this process on its own as an organization that eschews top-down regulation of this type, it can and is required to respond to community calls for such a reporting system, which clearly falls within its bylaws remit.

The domain registry and registrar community stands ready, alongside organizations including our own, to begin this process. CISA should prioritize working with these DNS entities and organizations to harmonize global reporting efforts.

By advancing this approach, the Internet community can set a precedent for international cooperation in cybersecurity, demonstrating how global challenges can be addressed through coordinated efforts.

Para. 48: How should the U.S. government's support for the multi-stakeholder system of internet governance inform the DNS exception?

The U.S. government's support for the multi-stakeholder system of Internet governance, as articulated within the Declaration of the Future of the Internet,[10] validates the adoption by CISA of a Final Rule with a broader scope for the DNS Exception. The multi-stakeholder model, which allows for participation by all categories of necessary stakeholders, including governments, industry, civil society, academia, and technical experts, has been fundamental to developing and maintaining a secure and stable global, open, and interoperable Internet.

1. Consistency with Principles of Multi-Stakeholder Governance. The DNS Exception should align with the principles of multi-stakeholder governance by recognizing the unique roles and responsibilities of different stakeholders in managing the DNS ecosystem. It should acknowledge the expertise and input of stakeholders such as domain registries, registrars, technical operators, and the broader Internet community in shaping policies and practices related to cybersecurity and incident reporting.

2. Recognition of ICANN's Role. ICANN, as the global coordinator of the DNS, operates under a multi-stakeholder governance model. Its policies and procedures are developed through a bottom-up, consensus-driven process involving diverse stakeholders. The DNS Exception should respect ICANN's authority and role in overseeing domain name management and DNS operations, ensuring that any reporting requirements do not undermine ICANN's multi-stakeholder governance framework.

3. Promotion of Global Cooperation. The U.S. government's continued support for the multi-stakeholder system, which it helped to architect, underscores the importance of global cooperation in addressing cybersecurity challenges. CISA's implementation of the DNS Exception should encourage collaboration among stakeholders at the international level, fostering information sharing, capacity

[10] Declaration for the Future of the Internet https://www.state.gov/declaration-for-the-future-of-the-internet

building, and joint efforts to combat cyber threats effectively. It should facilitate partnerships between governments, industry, academia, and civil society to promote a globally coordinated approach to incident reporting and response.

4. Preservation of Innovation and Flexibility. The multi-stakeholder model promotes innovation, flexibility, and adaptability in Internet governance. The DNS Exception, when implemented, should reflect these principles by allowing for the development of tailored reporting mechanisms that suit the diverse needs and operational realities of different stakeholders. It should avoid imposing overly prescriptive or burdensome requirements that stifle innovation and hinder the ability of stakeholders to respond effectively to emerging global cyber threats.

5. Emphasis on Transparency and Accountability. Transparency and accountability are core principles of the multi-stakeholder model. The DNS Exception's implementation should promote transparency in the development and execution of reporting requirements, ensuring that stakeholders have access to relevant information and can participate meaningfully and in a timely manner in decision-making processes. It should also establish mechanisms for accountability, enabling stakeholders to monitor compliance and hold relevant parties accountable for their actions.

Para. 49: Any other aspects of CISA's proposed approach to the DNS exception.

CISA's proposed implementation of the DNS Exception has created some concern about the logical coherence of the exception criteria and raised questions about consistency. For example, Root Server Operators, to be exempted under the current framework, share many characteristics with domain registries and registrars, suggesting a logical basis for the inclusion of registries and registrars in the DNS Exception as well.

As CISA reviews its approach, it is essential to recognize the similarities between the entities already exempted in the Proposed Rule and domain registries and registrars. Root Server Operators, like domain registries and registrars, play a fundamental role in the DNS ecosystem, providing critical

services that underpin Internet functionality. They operate under similar governance frameworks and face comparable cybersecurity challenges.

Given these parallels, the DNS Exception should be extended in its implementation to domain registries and registrars based on the rationale already applied to exempt entities in the Proposed Rule. Including domain registries and registrars in the Exception aligns with the principles of consistency and fairness, ensuring that entities with similar characteristics are treated equitably under the exception framework.

Furthermore, extending the DNS Exception to domain registries and registrars enhances the coherence and stability of the exception framework. It eliminates potential discrepancies and uncertainties, providing clarity and predictability for stakeholders. By adopting a consistent approach to how the DNS Exception is applied, CISA can strengthen the resilience and stability of the DNS ecosystem.

III. CONCLUSION

Domain name registries and registrars should be deemed by CISA in the Final Rule to be within the scope of the DNS Exception due to their critical role in operating inherently global Internet infrastructure and their governance under ICANN's multi-stakeholder framework. Applying this exception to all of the core DNS services and technical functions these entities provide will streamline cyber incident reporting, reduce regulatory burdens, and enhance the security and stability of the global DNS. The overall ecosystem of the DNS, governed by ICANN, constitutes critical infrastructure,

underscoring the need for a cohesive and unified global approach to cybersecurity reporting and resilience.

Respectfully submitted,

Christian Dawson, Executive Director
Ann Morton, Senior Policy Director
Internet Infrastructure Coalition
2920 W. Broad Street, Suite 80
Richmond, VA 23230
dawson@i2coalition.com
ann@i2coalition.com

July 3, 2024