

DNS ABUSE

ICANN New gTLD Program — Round 2026

Application Question Q221 (Q5.2-1) — All Financial Profiles

Reference: *Applicant Guidebook V1-2025.12.16 — DNS Abuse Evaluation, Operational Evaluation, Question Set 19 (Q221). ICANN defines DNS Abuse as: Phishing, Malware, Botnets, Pharming, and Spam (when used as a delivery mechanism for the preceding forms of abuse).*

APPLICANT IDENTIFICATION

Applying Entity (full legal name): Two Sigma Investments, LP

Jurisdiction of incorporation: Delaware, USA

Applied-for gTLD string(s): .twosigma

Registry Services Provider (RSP): Afnic

SELF-CERTIFICATION STATEMENTS

The applying entity hereby certifies the following statements in connection with the operation of the applied-for gTLD, .twosigma:

Statement 1 — Dedicated Abuse Point of Contact (SC5.2-1.1)

The applying entity will, no later than delegation of the Top Level Domain (TLD), establish a dedicated abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning any name registered in the TLD.

Statement 2 — Abuse Reporting Mechanism (SC5.2-1.2)

The applying entity will, no later than delegation of the TLD, establish, publish, and provide to ICANN the location of a mechanism for members of the public to submit reports of abuse in accordance with the current obligations of the Base RA and any Consensus Policies.

Statement 3 — Orphan Glue Record Removal (SC5.2-1.3)

The applying entity has developed proposed measures for removal of orphan glue records for names removed from the zone when provided with evidence in written form that the glue is present in connection with malicious conduct (see Specification 6).

Statement 4 — Public Abuse Policies (SC5.2-1.4)

The applying entity has or will have at time of delegation, established policies for handling complaints regarding abuse. Such policies are to be maintained and posted publicly so that anyone can review the policies via the Internet and any other means deemed appropriate by the applying entity. The applying entity's policies at a minimum should contain appropriate confirmation of the receipt of the abuse report, the process of review of the report, and actions that will be taken if the applying entity confirms the report is legitimate.

Statement 5 — Understanding of DNS Abuse Types (SC5.2-1.5)

The applying entity understands that DNS Abuse is Phishing, Malware, Botnets, Pharming and Spam (when used to deliver other forms of DNS Abuse). The applying entity understands and is prepared to contribute to the mitigation or disruption of DNS Abuse in domains in the TLD zone.

Statement 6 — Abuse Response Capabilities (SC5.2-1.6)

The applying entity's abuse response capabilities are resourced appropriately to ensure a timely and adequate investigation and response to reports of DNS Abuse. This includes capabilities to receive and evaluate evidence of DNS Abuse in reports, and to take action to stop or disrupt the DNS Abuse.

Statement 7 — Periodic Zone Scans (SC5.2-1.7)

The applying entity is prepared to conduct periodic scans of its zone to identify if domains are being used to perpetrate DNS Abuse, and to maintain statistical reports of the scans, the findings, and actions taken.

SIGNATURES

By signing below, the undersigned confirms that the self-certification statements are true and accurate to the best of his knowledge.

Authorized Officer — Applying Entity

Full name: Jeff Wecker

Title / Position: Chief Technology Officer

Date: 07/15/2026

Signature:  _____