Response to Documentary Information Disclosure Policy Request

To: Michael Palage

Date: 28 September 2016

Re: Request No. 20160829-1

Thank you for your Request for Information dated 29 August 2016 (Request), which was submitted through the Internet Corporation for Assigned Names and Numbers (ICANN) Documentary Information Disclosure Policy (DIDP). Because your Request was submitted as part of an email that contained matters other than a DIDP request, the Request will not be published separately, but is set forth verbatim below. This Response will be published as a Request and Response to DIDP Request No. 20160829-1.

Items Requested

Your Request seeks the disclosure of "any documents in ICANN's possession, including but not limited to studies, reports, analysis, white papers, etc. addressing the topics of malware, spam, bots, cybersquatting, malicious/illegal activity etc. in connection with the domain name system (legacy gTLD Registries & Registrars, new gTLD Registries & Registrars, and ccTLDs Registries & Registrars) over the last three years."

Response

ICANN facilitates the security, stability and resiliency of the Internet's unique identifier systems through coordination and collaboration. The goal of ICANN's Identifier Systems Security, Stability, Resiliency (IS-SSR) programs and team (Security Team) is to support improvements in the security, stability and resiliency of the Domain Name System (DNS). As explained on ICANN's website (available at https://www.icann.org/resources/pages/is-ssr-2014-11-24-en), to achieve this goal, ICANN will:

- Engage actively with security, operations, and public safety communities to gather and process intelligence data that indicate (imminent) threats to the DNS or domain registration service operations (the "DNS ecosystem").
- Facilitate or participate with these same communities in threat preparedness activities to protect against or mitigate threats to the DNS ecosystem.
- Perform studies or analyze data to better understand the health and well-being of the DNS ecosystem.
- Coordinate DNS vulnerability disclosure reporting. (Report available at https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf.)
- Lend subject matter expertise to build capability among ccTLD and public safety communities in subjects relevant to the DNS ecosystem, including DNSSEC, abuse or misuse of DNS infrastructures or operations.
- Assist in DNS ecosystem risk management activities.

- With ICANN's Global Stakeholder Engagements team, participate in a global, multi-stakeholder effort to improve cybersecurity and mitigate cybercrime.

Extensive information regarding the Security Team and IS-SSR programs is publicly available on ICANN's website. (See https://www.icann.org/resources/pages/is-ssr-2014-11-24-en and https://www.icann.org/news/blog/what-is-icann-iis-ssr.) The Security Team provides thought leadership in the form of white papers, blog posts, and the annual Security, Stability & Resiliency Framework for ICANN. Blog posts by Security Team members regarding security threats as well as raising security awareness, dating from 2007 through 2016, are available at https://www.icann.org/resources/pages/is-ssr-blogs-2015-12-16-en and https://www.icann.org/resources/pages/security-terminology-2015-09-16-en. The ICANN IS-SSR Plans and Frameworks for FY10 through FY15-16 are available at https://www.icann.org/ssr-document-archive. In addition, papers, articles, SSR Symposium reports, Situation Awareness Bulletins, and Internet Governance & Cybersecurity documents are posted by the Security Team at https://www.icann.org/ssr-document-archive. Security Team members also represent ICANN at various conferences and events worldwide speaking on cybersecurity and governance. For example, the transcript and presentation materials of ICANN's Security Team – Outreach Session on 25 June 2014 is available at https://london50.icann.org/en/schedule/wed-ssr/presentation-ssr-25jun14-en. As the Security Team develops additional materials, reports, blogs, and papers relating to security threats, such documentation will be posted at the webpages noted above.

Further documents responsive to your Request are also publicly available through additional ICANN webpages. For instance, the Security and Stability Advisory Committee (SSAC) advises the ICANN community and the ICANN Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational, administrative, and registration matters. The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. Extensive information regarding the SSAC, including its Charter, correspondence, documents, discussions, projects, links to security-related posts, and the SSAC's work plans and Activity Reports, is available at https://www.icann.org/groups/ssac. In particular, the SSAC produces Reports, Advisories, and Comments on a range of topics that include, among other things, DNS Security and DNS Abuse. These SSAC documents are available at https://www.icann.org/groups/ssac/documents-by-category.

In addition, the Governmental Advisory Committee (GAC) Beijing Communiqué contained GAC Advice to the ICANN Board, noting that a number of safeguards should be applicable to all new gTLDs. The New gTLD Program Committee (NGPC) passed Resolution 2013.06.25.NG02 – 2013.06.25.NG03 (see https://www.icann.org/resources/board-material/resolutions-new-gtld-2013-06-25-en#2.b), adopting the "NGPC Proposal for Implementation of GAC Safeguards Applicable to All New gTLDs," which included proposed language to the New gTLD Registry Agreement (RA). Pursuant to the NGPC's Resolution, ICANN included a provision in the RA (as a mandatory Public Interest Commitment in Specification 11) requiring Registry Operators periodically to conduct a technical analysis to assess whether domains in their respective gTLDs are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Specification 11 also requires

Registry Operators to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks, and to provide these reports to ICANN upon request. The language of Specification 11 does not contain language for how Registry Operators ought to respond to identified security threats. As such, the NGPC Resolution (Annex I) further directed ICANN to solicit community participation to develop a framework for Registry Operators to respond to identified security risks that pose an actual risk of harm. (See https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-i-agenda-2b-25jun13-en.pdf.) As a result, ICANN has formed a Framework Drafting Team composed of volunteers from affected parties to draft a "Framework for Registry Operators to Respond to Security Threats" (Framework). Registries, Registrars, and GAC representatives (including from the Public Safety Working Group) have been invited to join the drafting effort. Information regarding the background, objectives, drafting principles, timeline and meetings log related to the Framework drafting is available at https://community.icann.org/display/S1SF/Security+Framework+Home. The current draft of the Framework is publicly available at https://community.icann.org/display/S1SF/Meetings+Log?preview=/54692000/62393503/Security%20Framwork%20-%20PSWG%20Input%20-%2020sep16%20-%20redlines.pdf. A final draft Framework will be submitted to the community for public comment; community input will then be considered by the drafting team to produce a finalized Framework for publication and implementation by interested parties.

To the extent there are other documents that may be responsive to your Request, they are subject to the following DIDP Defined Conditions for Nondisclosure:

- Information provided by or to a government or international organization, or any form of recitation of such information, in the expectation that the information will be kept confidential and/or would or likely would materially prejudice ICANN's relationship with that party.
- Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.
- Information exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates that, if disclosed, would or would be likely to compromise the integrity of the deliberative and decision-making process between and among ICANN, its constituents, and/or other entities with which ICANN cooperates by inhibiting the candid exchange of ideas and communications.
- Confidential business information and/or internal policies and procedures.
- Drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication.

- Information requests: (i) which are not reasonable; (ii) which are excessive or overly burdensome; (iii) complying with which is not feasible; or (iv) are made with an abusive or vexatious purpose or by a vexatious or querulous individual.

Notwithstanding the applicable Defined Conditions of Nondisclosure identified in this Response, ICANN also evaluated the documents subject to these conditions to determine if the public interest in disclosing them outweighs the harm that may be caused by such disclosure. ICANN has determined that there are no particular circumstances for which the public interest in disclosing the information outweighs the harm that may be caused by the requested disclosure.

About DIDP

ICANN's DIDP is limited to requests for documentary information already in existence within ICANN that is not publicly available. In addition, the DIDP sets forth Defined Conditions of Nondisclosure. To review a copy of the DIDP, please see http://www.icann.org/en/about/transparency/didp. ICANN makes every effort to be as responsive as possible to the entirety of your Request. As part of its accountability and transparency commitments, ICANN continually strives to provide as much information to the community as is reasonable. We encourage you to sign up for an account at MyICANN.org, through which you can receive daily updates regarding postings to the portions of ICANN's website that are of interest because, as we continue to enhance our reporting mechanisms, reports will be posted for public access.

We hope this information is helpful. If you have any further inquiries, please forward them to didp@icann.org.