Response to Documentary Information Disclosure Policy Request

To: Geetha Hariharan

Date: 23 January 2015

Re: Request No. 20141224-1

Thank you for your Request for Information dated 24 December 2014 (the "Request"), which was submitted through the Internet Corporation for Assigned Names and Numbers' (ICANN) Documentary Information Disclosure Policy (DIDP) on behalf of The Centre for Internet & Society (CIS). For reference, a copy of your Request is attached to the email forwarding this Response.

Items Requested

Your Request seeks the disclosure of "details of all cyber-attacks suffered or thought/suspected to have been suffered by ICANN (and for which, therefore, investigation was carried out within and outside ICANN), from 1999 till date." Your Request specified that the responsive documents include the following items:

(1) the date and nature of all attacks, as well as which ICANN systems were compromised;

(2) actions taken internally by ICANN upon being notified of the attacks;

(3) what departments or members of staff are responsible for security and their role in the event of cyber-attacks;

(4) the role and responsibility of the ICANN-CIRT in responding to cyber attacks (and when policies or manuals exist for the same; if so, please share them);

(5) what entities external to ICANN are involved in the identification and investigation of cyber-attacks on ICANN (for instance, are the police in the jurisdiction notified and do they investigate? If so, produce copies of complaints or information reports);

(6) whether and when culprits behind the ICANN cyber-attacks were identified; and

(7) what actions were subsequently taken by ICANN (ex: liability of ICANN staff for security breaches should such a finding be made, lawsuits or complaints against perpetrators of attacks, etc.)."

Response

ICANN's DIDP is intended to "ensure that information contained in documents concerning ICANN's operational activities, and within ICANN's possession, custody, or control, is made available to the public unless there is a compelling reason for confidentiality." (*See* https://www.icann.org/resources/pages/didp-2012-02-25-en (emphasis added).) As part of its approach to transparency and information disclosure, ICANN makes available on its website at www.icann.org a comprehensive set of materials concerning ICANN's operational activities as a matter of course, including, but not limited to, the following categories of documents: Annual Reports, Articles of Incorporation, Board meeting transcripts, minutes and resolutions, budget, Bylaws (current and archives), correspondence, financial information, litigation documents, major agreements, monthly Registry reports, Operating Plan, policy documents, speeches, presentations and publications, Strategic Plan, material information relating to the SOs/ACs. ICANN also continually assesses the ways in which it can enhance its reporting mechanisms by improving upon the levels of reporting where feasible.

Further as part of its commitment to openness and transparency, ICANN makes publicly available on its website information regarding cybersecurity, including information regarding cyber attacks on ICANN's systems. (*See* "ICANN Targeted in Spear Phishing Attack; Enhanced Security Measures Implemented" available at https://www.icann.org/news/announcement-2-2014-12-16-en; "ICANN Identifier System SSR Update – 2H 2014" available at https://www.icann.org/en/system/files/files/is-ssr-update-s2-2014-21jan15-en.pdf; "The Heartbleed Bug: Are you at risk?" available at http://blog.icann.org/category/dns/page/2/.) Information regarding cybersecurity can be found on the Identifier Systems Security, Stability and Resiliency (IS-SSR) page at https://www.icann.org/resources/pages/is-ssr-2014-11-24-en, the Security Team page at https://www.icann.org/resources/pages/security-2012-02-25-en, the Computer Incident Response Team (CIRT) page at https://www.icann.org/resources/pages/cirt-2012-02-25-en, the Security Awareness page at https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en, the ICANN Blog at https://www.icann.org/news/blog, the Announcements page at https://www.icann.org/news/announcements; and the Security and Stability Advisory Committee (SSAC) page at https://www.icann.org/resources/pages/ssac-2012-02-25-en including SSAC Report No. SAC007 "Domain Name Hijacking Report" (https://www.icann.org/announcements/hijacking-report-12jul05.pdf) and Report No. SAC040 "Measures to Protect Domain Registration Services Against Exploitation and Misuse" (https://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf).

Your Request seeks the disclosure of "details of all cyber-attacks suffered or thought/suspected to have been suffered by ICANN (and for which, therefore, investigation was carried out within and outside ICANN), from 1999 till date." Your Request specified that the responsive documents include the information set forth in Items 1 through 7 identified above under "Items Requested".

Your Request is vague and overbroad in time and scope in so far as the term "cyber-attack" is undefined. As stated in your Request, the term "cyberattacks" is very broad and includes "all cyber-attacks suffered or thought/suspected to have been suffered by ICANN" without any distinction between successful or attempted attacks. Nor does your Request distinguish between information security incidents versus events.

According to the ISO 27001 standard, an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant where an information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. Most corporations experience information security events on a regular basis. ICANN is no exception. These events do not necessarily result in a direct impact on ICANN's systems and can often be easily triaged.

ICANN does not compile and maintain, in the normal course of business, documents regarding each security "event" suffered or thought/suspected to have been suffered by ICANN containing the information specified in Items 1 through 7. As such, ICANN's search for documents responsive to this Request revealed that no such responsive documents exist within ICANN. As noted above, ICANN's DIDP is intended to ensure that documents concerning ICANN's operational activities, and within ICANN's possession, custody, or control, are made available to the public unless there is a compelling reason for confidentiality. Accordingly, a threshold consideration in responding to a DIDP request, then, is whether the documents requested are in ICANN's possession, custody, or control. Under the DIDP, where the responsive document does not exist, ICANN shall not be required to create or compile summaries of any documented information. (*See* https://www.icann.org/resources/pages/didp-2012-02-25-en.)

ICANN has already made publicly available documents relevant to your Request regarding security "incidents" for which internal and investigations were conducted including the attacks on the ICANN and IANA websites and the ICANN blog that occurred in June 2008 (*see* "Response to Recent Security Threats" at https://www.icann.org/news/announcement-2008-07-03-en; SSAC Report No. SAC007 "Domain Name Hijacking Report" at https://www.icann.org/announcements/hijacking-report-12jul05.pdf); and SSAC Report No. SAC040 "Measures to Protect Domain Registration Services Against Exploitation and Misuse" at https://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf) and the spear phishing attack that occurred in late November 2014 (*see* "ICANN Targeted in Spear Phishing Attack: Enhanced Security Measures Implemented" at https://www.icann.org/news/announcement-2-2014-12-16-en). Additionally, while it was not a direct attack on ICANN, ICANN has published documents containing information about the attack on the root server system incident that occurred on 6 February 2007, including information regarding the nature of the attack and the systems affected. (*See* https://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf;

http://blog.icann.org/2007/03/factsheet-dns-attack/.) Where available, practicable and feasible, the information provided in these documents includes the date and nature of the attacks (Item No. 1), actions taken by ICANN upon being notified of the attacks (Item No. 2), and the parties behind the attacks (Item No. 6).

With respect to Item No. 3, the members of the ICANN Security Team and their roles are identified on the Security Team page at https://www.icann.org/resources/pages/security-2012-02-25-en. With respect to Item No. 4, information regarding the role and responsibility of the ICANN-CIRT in responding to cyber attacks is available on the CIRT page at https://www.icann.org/resources/pages/cirt-2012-02-25-en.

Subject to the publicly available documents relevant to your Request, your Request is subject to the following DIDP Defined Conditions of 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.
- Confidential business information and/or internal policies and procedures.

- Information subject to the attorney– client, attorney work product privilege, or any other applicable privilege, or disclosure of which might prejudice any internal, governmental, or legal investigation.

- 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; and (iii) complying with which is not feasible.

About DIDP

ICANN's DIDP is limited to requests for 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, which is contained within the ICANN Accountability & Transparency: Framework and Principles 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.