January 7, 2016

Mr. Nathan Paul Mehrens
President and General Counsel
Americans for Limited Government Foundation
10332 Main Street, No 326
Fairfax, VA 22030

      RE: NTIA FOIA 015-062

Dear Mr. Mehrens:

On July 15, 2015, the National Telecommunications and Information Administration (NTIA), Office of the Chief Counsel, received a request under the Freedom of Information Act (FOIA), as amended (5 U.S.C. § 552). In this request, you sought:

- All records relating to communications between the National Telecommunications and Information Administration (NTIA) and the Internet Corporation for Assigned Names and Numbers (ICANN) and Verisign regarding Administrative Functions Associated with Root Zone Management pursuant to Section C.2.9.2 of the contract between NTIA and ICANN that became effective on October 1, 2012. Provide all such records that were created on or after October 1, 2012 [until July 15, 2015].

On that same date, NTIA acknowledged receipt of this FOIA and agreed to proceed accordingly.

As a part of this request, you also sought a fee waiver. On August 12, 2015, NTIA denied your request for a fee waiver and provided a fee estimate in the amount of $3,150.79. On September 21, 2015, NTIA received a modification of the original request and a supplement to your fee waiver and media requests. Your modified request is now as follows:

- All records relating to communications between the National Telecommunications and Information Administration (NTIA) and the Internet Corporation for Assigned Names and Numbers (ICANN) and Verisign regarding Administrative Functions Associated with Root Zone Management pursuant to Section C.2.9.2 of the contract between NTIA and ICANN that became effective on October 1, 2012, excluding (1) all records that have been previously released to the public; and (2) administrative email that are referred to in Footnote 9 of the letter to me from Kathy D. Smith dated August 12, 2015.

On September 22, 2015, NTIA granted your request for a fee waiver. Enclosed, please find the first interim response to your request. This response contains ten electronic files. These records are being released in their entirety.

NTIA has designated this request as complex and are processing it accordingly and will continue to provide you with records on a rolling basis as you have agreed. NTIA has also extended the time to complete this request beyond the normal twenty days due to unusual circumstances, including the need to send records for business confidential review to the original submitters and for the volume of records involved. If you have any questions regarding the processing of your request, please contact Stacy Cheney, Senior Attorney Advisor, at 202-482-1864 or via email at scheney@ntia.doc.gov.

Sincerely,
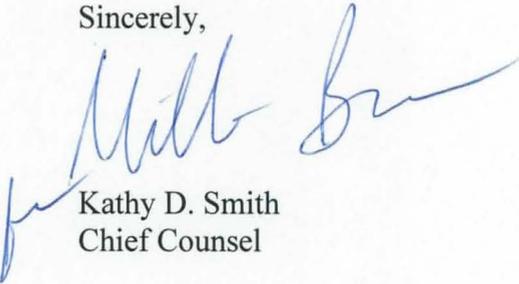
Kathy D. Smith
Chief Counsel

To recap next steps identified on our call today:

* NTIA to provide redlines on the draft consultation by COB this Friday (12/20) and circulate to the group. Intent is to keep consultation as focused as possible to the matter at hand. NTIA general observation is that there is a bit of info currently included that doesn't obviously tie back to the purpose of consultation and/or may trigger unsolicited chatter/input.
* Joe/Tomofumi to provide revised version by COB 1/8/13.
* Next call will be at usual time on Wednesday 1/9/13.

Milestone/Dates to strive for:

* NTIA "blessed" consultation; January 15, 2013
* ICANN consultation initiated; January 31, 2012

-----Original Message-----
From: Joe Abley [mailto:joe.abley@icann.org]
Sent: Tuesday, December 18, 2012 4:23 PM
To: Ashley Heineman
Cc: Tomofumi Okubo; Verd Brad; Vernita D. Harris; Larson Matt; Duane Wessels (dwessels@verisign.com)
Subject: Re: DNSSEC Weekly Call

On 2012-12-18, at 15:55, Ashley Heineman <AHeineman@ntia.doc.gov> wrote:

> Thanks Joe. Thought TCR discussion was off the table until after the new year, but happy to discuss.

Oh, right. Just making sure we hadn't forgotten about it. No problems with waiting until January.

> Cool as well on other points, including possible need to be muted. :-)

I make the most sense when I'm muted :-)

Joe

From:	Ashley Heineman
To:	Joe Abley
Subject:	DNSSEC Consultation format
Date:	Thursday, January 10, 2013 2:26:00 PM

Hi Joe. Just wanted to close the loop on the "format" discussion. I spoke to Vernita last night. I think the best way to proceed is for NTIA to wait for your next revision and if there are any formatting issues… we'll address in our comments back. Sound good?

From:	Fiona Alexander
To:	Suzanne Radell; Elizabeth Bacon; Ashley Heineman
Cc:	Vernita D. Harris
Subject:	FW: Letter sent to VeriSign this afternoon
Date:	Friday, August 02, 2013 4:50:36 PM
Attachments:	Kane Ltr - Aug_2_13.pdf

Just so everyone is aware of the final.

From: Fiona Alexander
Sent: Friday, August 02, 2013 4:50 PM
To: Larry Strickling; Angela Simpson; Heather Phillips; Jim Wasilewski
Cc: Jade Nester; Cyril J. Dadd; Sara Morris; Juliana Gruenwald
Subject: Letter sent to VeriSign this afternoon

The attached was just sent. While we don't post our website or generally make correspondence public there is always the chance it will get out and in fact with ICANN copied they may naturally post on their website. If we hear any chatter we'll let folks know.

Mr. Patrick S. Kane   **AUG 0 2 2013**
Senior Vice President
VeriSign Naming and Directory Services
12061 Bluemont Way
Reston, VA 20190

Dear Mr. Kane:

I am writing in response to your letter of May 30, 2013, raising concerns related to the root zone system and the addition of new generic top-level domains (gTLDs). Through the Cooperative Agreement (*Agreement*) between the National Telecommunications and Information Administration (NTIA) and VeriSign, VeriSign serves as the Root Zone Maintainer, operator of the "A" Root Server, and registry operator for .com, all of which have, to date, been integral to ensure the stability and security of the domain name system (DNS). We are very surprised to receive your letter given your previous public statements, including the joint statement of the root zone partners last November that VeriSign was prepared to deploy new gTLDs into the root at the rate of at least 100 per week.

In response to your claims now that critical issues must be addressed before you are ready to implement the new gTLD program, you are no doubt aware that the Root Server Stability Advisory Committee (RSSAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) is right now developing requirements of root server system monitoring, instrumentation, and management capabilities as well as the establishment of an early warning capability. The RSSAC has captured in RSSAC001 "*Service Expectations of Root Servers,*" a set of service expectations that root server operators must satisfy. In addition, through RSSAC002 "*RSSAC Recommendations on the measurement of the Root Server System,*" the RSSAC has developed the parameters for the basis of an early warning system that will assist in detecting and mitigating any effects (or the absence of such effects) that would challenge the scaling and/or working of the Internet's DNS root server system as a result of new gTLDs. NTIA understands these documents are in the final stages of approval and will be formally submitted to the ICANN Board in the coming weeks. Given Verisign's role as a key member of RSSAC, we expect and encourage your active participation and leadership in concluding this work in time for the launch of the new gTLD program within the time frame articulated by ICANN's senior management.

Within the last five years, ICANN, VeriSign and NTIA, working collaboratively, have made significant changes to the DNS root zone and the management systems. For instance, on June 16, 2010, an important milestone was achieved with the successful deployment of Domain Name System Security Extensions (DNSSEC). Furthermore, the deployment of the root zone management automation (RZM) system on July 21, 2011, and further enhancements made to the RZM system on May 16, 2013, improved the end-to-end process for root zone management. These changes entailed a certain risk to the stability of the DNS, but by working together, we

demonstrated that we could manage these risks and in fact, we implemented DNSSEC without any harm to the root zone.

The root zone partners have demonstrated their ability to mitigate the risks associated with executing an emergency change request with appropriate authorizations in an accelerated time frame. Therefore, the checks put in place today in the automated system, and the ability to exercise an emergency authorization to revert to previous root zone data for automation would be sufficient for the delegation of new gTLDs. If in the longer term, VeriSign believes an explicit policy and operational framework is needed to codify the halting of or rollback of delegations within the root, we would encourage you to pursue such an effort within the appropriate ICANN multistakeholder processes.

NTIA and VeriSign have historically had a strong working relationship, but inconsistences in VeriSign's position in recent months are troubling. Given your obligations under the *Agreement*, NTIA fully expects VeriSign to process change requests when it receives an authorization to delegate a new gTLD. So that there will be no doubt on this point, please provide me written confirmation no later than August 16, 2013 that VeriSign will process changes requests for the new gTLD program when authorized to delegate a new gTLD.

Sincerely,
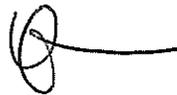
Vernita D. Harris

cc: Ms. Elise Gerich, Vice President, ICANN

From:	Fiona Alexander
To:	Theresa Swinehart; Kane, Pat
Cc:	grace.abuhamad@icann.org; Drazek, Keith (kdrazek@verisign.com); Jamie Hedlund (jamie.hedlund@icann.org); Ashley Heineman
Subject:	FW: NTIA Review of IANA Root Zone Change Requests
Date:	Tuesday, November 18, 2014 12:23:57 PM

FYI on this. Once we have something pulled together we will touch base with you before distributing.

From: Fiona Alexander
Sent: Tuesday, November 18, 2014 12:22 PM
To: 'Allan MacGillivray'
Cc: Ashley Heineman
Subject: RE: NTIA Review of IANA Root Zone Change Requests

Hi Allan

As I'm sure you are aware we have in the past described our role as clerical and verifying that appropriate processes have been followed. Beyond that we do not currently have an off the shelf document to offer, but take the point you raise below and are currently working on something to send to inform the group's discussion. NTIA's goal is get that out as soon as possible. Thanks for directly raising the issue with us.

Fiona

Fiona M. Alexander

Associate Administrator for International Affairs

National Telecommunications and Information Administration (NTIA)

(202) 482-1866

www.ntia.doc.gov

From: Allan MacGillivray [mailto:allan.macgillivray@cira.ca]
Sent: Monday, November 17, 2014 3:24 PM
To: Fiona Alexander
Subject: NTIA Review of IANA Root Zone Change Requests

Fiona – you may know that the naming community's cross community working group on IANA transition is meeting F2F in Frankfurt this week (Tuesday night to Thursday). We are very much trying to meet the timeline that has been set out by NTIA for a transition proposal so we will need to effectively complete a draft for the naming community this week if we are to meet the schedule that the ICG has set.

One piece of valuable information we lack is a better understanding of the process that NTIA staff go through upon receipt of a request from IANA to change the Root Zone before instructing

Verisign, as Root Zone Maintainer, to effect the change. This information goes to the question of specifically what functions will need to be replaced were NTIA staff no longer part of the process. Very little is known about just how substantive the NTIA review of the IANA requests currently is. Apparently there is some form of 'checklist' that NTIA staff follow. Would you be able to share this with us?

Thank you

Allan MacGillivray (.ca) on behalf of RFP3, Naming CWG

FYI

ICANN News Alert

https://www.icann.org/news/announcement-2014-12-19-en

_____

IANA Systems Not Compromised

19 December 2014

As ICANN reported on 16 December 2014, it was recently the target of a so-called "spear phishing" attack. During this attack the email credentials of some ICANN staff were compromised.

As mentioned in our original announcement (https://www.icann.org/news/announcement-2-2014-12-16-en), we have confirmed that the attack has not impacted any IANA-related systems. The ICANN staff members whose passwords were compromised did not have access to the IANA functions systems.

The IANA functions are a separate system with additional security measures that have not been breached.

During and after the attack, all critical functions hosted by hosted by ICANN, including the IANA functions, remained fully operational and unaffected by the attacker's activities.

ICANN employs multiple levels of protection for its most critical services. While the attackers were able to breach the outermost layer of defenses, our on-going investigation indicates our most critical systems were not affected.

_____

Hi Juliana,

Hit reply to soon. Perhaps we lead with the IANA systems were not impacted….. and the IANA functions contract…

Is this helpful?

From: Vernita D. Harris
Sent: Friday, December 19, 2014 10:39 AM
To: Juliana Gruenwald
Cc: Heather Phillips
Subject: RE: proposed answer

The IANA-related systems were not impacted by the ICANN security breach. However, the IANA Functions Contract does require ICANN to operate in accordance with best business and security practices. This includes ensuring the information systems have effective security safeguards and notifying NTIA in the case of breach or outage. As this breach did not impact the IANA-systems, ICANN is best placed to answer questions associated with this incident.

From: Juliana Gruenwald
Sent: Friday, December 19, 2014 10:35 AM
To: Vernita D. Harris
Cc: Heather Phillips
Subject: RE: proposed answer

I would rather not. Isn't the contract public?

From: Vernita D. Harris
Sent: Friday, December 19, 2014 10:34 AM
To: Juliana Gruenwald
Cc: Heather Phillips
Subject: RE: proposed answer

Hi Juliana,

This is okay. Can we run this by OCC to make sure they are comfortable with the text?

--Vernita

From: Juliana Gruenwald
Sent: Friday, December 19, 2014 10:22 AM
To: Vernita D. Harris
Cc: Heather Phillips

Subject: RE: proposed answer

Ok, just to be clear, this is what I will plan to send the repoter. Let me know if its OK:

On background:

The IANA Functions Contract requires ICANN to operate in accordance with best business and security practices. This includes ensuring the information systems have effective security safeguards and notifying NTIA if there is a breach or outage. ICANN did inform us of the breach and assured NTIA that the IANA-related systems were not impacted. You must contact ICANN for any other questions related to the incident itself.

From: Vernita D. Harris
Sent: Friday, December 19, 2014 10:19 AM
To: Juliana Gruenwald
Cc: Heather Phillips
Subject: RE: proposed answer

The Security Requirements were for your FYSA and not intended to be sent to Monica.

From: Juliana Gruenwald
Sent: Friday, December 19, 2014 9:59 AM
To: Vernita D. Harris
Cc: Heather Phillips
Subject: proposed answer

Hi – So here's a proposed response to those questions from that German reporter based on guidance from Larry and our convo. Can you just make sure its accurate? Thanks

On background:
ICANN is required under the IANA contract to ensure adequate cyber security and to notify NTIA if there is a breach. They did inform us of the breach and assured NTIA that the IANA functions were not impacted. You must contact ICANN for any other questions related to the incident itself.

Juliana Gruenwald
National Telecommunications and Information Administration (NTIA)
Phone: 202-482-2145
Email: jgruenwald@ntia.doc.gov

You have probably seen this already, but just in case.

From: Stacy Cheney
Sent: Friday, December 19, 2014 12:46 PM
To: Kathy Smith
Subject: FW: ICANN News Alert -- IANA Systems Not Compromised

FYI

From: ICANN News Alert [mailto:communications@icann.org]
Sent: Friday, December 19, 2014 12:00 PM
To: Stacy Cheney
Subject: ICANN News Alert -- IANA Systems Not Compromised

News Alert

https://www.icann.org/news/announcement-2014-12-19-en

IANA Systems Not Compromised

19 December 2014

As ICANN reported on 16 December 2014, it was recently the target of a so-called "spear phishing" attack. During this attack the email credentials of some ICANN staff were compromised.

As mentioned in our original announcement, we have confirmed that the attack has not impacted any IANA-related systems. The ICANN staff members whose passwords were compromised did not have access to the IANA functions systems.

The IANA functions are a separate system with additional security measures that have not been breached.

During and after the attack, all critical functions hosted by hosted by ICANN, including the IANA functions, remained fully operational and unaffected by the attacker's activities.

ICANN employs multiple levels of protection for its most critical services. While the attackers were able to breach the outermost layer of defenses, our on-going

investigation indicates our most critical systems were not affected.

-------- Original message --------
From: ICANN News Alert
Date:12/17/2014 12:43 AM (GMT-05:00)
To: Fiona Alexander
Subject: ICANN News Alert -- ICANN Targeted in Spear Phishing Attack | Enhanced Security Measures Implemented

ICANN

News Alert

https://www.icann.org/news/announcement-2-2014-12-16-en

ICANN Targeted in Spear Phishing Attack | Enhanced Security Measures Implemented

16 December 2014

ICANN is investigating a recent intrusion into our systems. We believe a "spear phishing" attack was initiated in late November 2014. It involved email messages that were crafted to appear to come from our own domain being sent to members of our staff. The attack resulted in the compromise of the email credentials of several ICANN staff members.

In early December 2014 we discovered that the compromised credentials were used to access other ICANN systems besides email:

- The Centralized Zone Data System (czds.icann.org)
  The attacker obtained administrative access to all files in the CZDS. This included copies of the zone files in the system, as well as information entered by users such as name, postal address, email address, fax and telephone numbers, username, and password. Although the passwords were stored as salted cryptographic hashes, we have deactivated all CZDS passwords as a precaution. Users may request a new password at czds.icann.org. We suggest that CZDS users take appropriate steps to protect any other online accounts for which they might have used the same username and/or password. ICANN is providing notices to the CZDS users whose personal information may have been compromised.

- The ICANN GAC Wiki (gacweb.icann.org)
  Public information, the members-only index page and one individual user's profile page was viewed. No other non-public content was viewed.

Unauthorized access was also obtained to user accounts on two other systems, the ICANN Blog (blog.icann.org) and the ICANN WHOIS (whois.icann.org) information portal. No impact was found to either of these systems.

Based on our investigation to date, we are not aware of any other systems that have been compromised, and we have confirmed that this attack does not impact any IANA-related systems.

Earlier this year, ICANN began a program of security enhancements in order to strengthen information security for all ICANN systems. We believe these enhancements helped limit the unauthorized access obtained in the attack. Since discovering the attack, we have implemented additional security measures.

We are providing information about this incident publicly, not just because of our commitment to openness and transparency, but also because sharing of cybersecurity information helps all involved assess threats to their systems.

For additional information about the attack, please monitor the ICANN website.

From:	Fiona Alexander
To:	Kathy Smith; Ashley Heineman; Vernita D. Harris
Subject:	FW: Following up
Date:	Monday, January 26, 2015 9:40:16 AM
Attachments:	image001.gif
	image002.jpg

Can you all make Reston on Friday?

From: Kane, Pat [mailto:pkane@verisign.com]
Sent: Monday, January 26, 2015 9:37 AM
To: Fiona Alexander
Subject: RE: Following up

Good morning Fiona,

I know that Tom and Kathy spoke on Friday. How about we get together this Friday out here in Reston? I don't believe that Kathy has seen the place.

Pat

Patrick Kane
Senior Vice President
Verisign Naming and Directory Services
PKane@Verisign.com

t: 703.948.3349
12061 Bluemont Way
Reston, VA 20190

VerisignInc.com The Manifesto of Done - The point of being done is not
to finish, but to get other things done.

From: Fiona Alexander [mailto:FAlexander@ntia.doc.gov]
Sent: Thursday, January 22, 2015 11:59 AM
To: Kane, Pat
Subject: Following up

Hi Pat

I hope the holidays were ok, all things considered. Again, please accept my condolences for your loss.

I'm writing to follow up on our conversations at the end of last year about the need for NTIA and Verisign to sit down and discuss the transition of our relationship in the root zone process that will need to happen as part of the stewardship transition. I think a conversation that includes Tom and Kathy would be useful. Can you check schedules and let me know what works on your end and if

you'd prefer a face to face meeting or a call.

Fiona