



UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-

APR 18 2014

Nate Cardozo
Staff Attorney
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

Dear Mr. Cardozo:

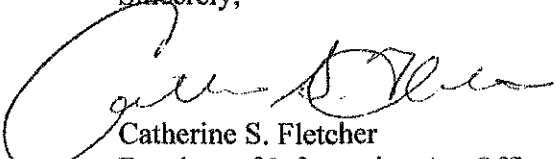
This letter is the first interim response to your February 3, 2014, Freedom of Information Act (FOIA) request (Log #DOC-NIST-2014-000488), with clarification* to the National Institute of Standards and Technology (NIST) in which you requested the following records:

- (1) "All records, emails and communications related to the participation of NIST or NSA employees in the development of the American National Standards Institute (ANSI) X9.82 standard for Random Number Generation from the period 2002 through 2007.
- (2) All records, emails and communications related to the participation of NIST or NSA employees in the development of NIST Special Publication 800-90, during the time period 2002 through 2007.
- (3) All unclassified records, emails, invoices and communications related to NSA's participation in the standardization of Suite B cryptography by the Internet Engineering Task Force, including the development of the following proposed standards: "Opaque PRF Inputs for TLS" and "Extended Random Values for TLS," authored by Eric Rescorla and Margaret Salter." *THE CLARIFIED SCOPE OF ITEM #3 IS FOR THE YEARS 2004-2010

NIST continues to conduct a search of our files responsive to your FOIA request. Enclosed you will find two (2) responsive documents consisting of four (4) pages that are being released in their entirety. NIST will continue to search for additional documents related to your request and send you releasable documents on a rolling basis as they become available.

Thank you for your patience.

Sincerely,



Catherine S. Fletcher
Freedom of Information Act Officer

Enclosures

NIST

Friday, February 21, 2014 10:42:46 AM Eastern Standard Time

Subject: Fwd: RE: Draft response to Bruce Schneier
Date: Monday, November 19, 2007 11:55:40 AM Eastern Standard Time
From: Curt Barker
To: ddodson@nist.gov, Burr, William E., ebarker@nist.gov

X-Sieve: CMU Sieve 2.3
From: "Gail Porter" <porter@nist.gov>
Reply-To: "gail.porter@nist.gov" <gail.porter@nist.gov>
To: "Ben Stein" <benjamin.stein@nist.gov>,
"Curt Barker"
<curt.barker@nist.gov>
CC: "gail.porter@nist.gov" <gail.porter@nist.gov>
Subject: RE: Draft response to Bruce Schneier
Date: Mon, 19 Nov 2007 10:01:17 -0500
Organization: NIST
X-Mailer: Oracle Connector for Outlook 10.1.1.0.2 70630 (11.0.8118)
X-Accept-Language: en-us, en
X-NIST-MailScanner: Found to be clean
X-NIST-MailScanner-From: porter@nist.gov
X-NIST-MailScanner-Information:

Ben:
One small but I think important suggested revision.
Thanks,
Gail

From: Ben Stein [<mailto:benjamin.stein@nist.gov>]
Sent: Monday, November 19, 2007 9:51 AM
To: 'Curt Barker'
Cc: gail.porter@nist.gov
Subject: Draft response to Bruce Schneier

Dear Curt,

Gail and I have come to the conclusion that we should initiate a response to the Schneier column. I'm thinking the best thing to do is to write him a letter (rather than send a letter directly to Wired, since this piece is online and may not make it into the print issue). The draft is attached. I have not yet designated the person who would sign the letter--feel free to send me a suggestion; otherwise I can sign it. We would send a finalized response to him, and then also send it to Wired. We'd also furnish it to any reporters who ask for our response. I'd also like to send it to the publications (such as Ars Technica and the Register) that have reported on his column.

We feel some response is warranted because it's an issue of public perception, image and reputation. This column could contribute to future misperceptions about NIST. We have the opportunity to make some valid points about the algorithm and to set the record straight.

I've given my counterparts at NSA a heads-up about our plans to do a response and I will send them the final letter as a courtesy.

Let me know if this works for you. After incorporating your comments, we could send the draft to Bill Burr for his comments, and afterwards to Mat and throughout the director's office. I'd be very happy to discuss this further.

Thanks,
Ben
x3097