



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

JAN 15 2015

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

Dear Mr. Cardozo:

This letter is the fourth interim response to your February 3, 2014, Freedom of Information Act (FOIA) request (#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 has located additional records responsive to your FOIA request. Enclosed you will find eleven (11) documents consisting of one-hundred-sixty-five (165) pages that are being released in their entirety.

Thank you for your patience. We will continue to send you releasable documents on a rolling basis as they become available.

Sincerely,

Catherine S. Fletcher
Freedom of Information Act Officer

Enclosures

NIST