The Honorable Patrick D. Gallagher
Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Mr. Gallagher:
My office has been in touch with Johns Hopkins Professor Matthew Green, a computer scientist with expertise in cryptography and privacy. Professor Green is concerned, based on public reports in the New York Times/ProPublica, about the possibility that National Institute of Standards and Technology (NIST) security standards have been intentionally weakened by the National Security Agency (NSA).
With this in mind, I have some questions:
1) Did the NSA request and NIST include a compromised random number generation algorithm called "Dual EC DRBG" in a NIST standard?

2) If so, why was the vulnerable standard -- which was released and later incorporated within the products of several major U.S. technology corporations, including Microsoft, Cisco and EMC - released despite the fact that experts notified NIST of concerns with the algorithm prior to the finalization of the standard (in approximately February 2006)?

3) Did NIST staff assist the NSA in working to include the algorithm into American National Standards Institute (ANSI) and International Organization for Standardization (ISO) standards?

In addition, please remit to my office the following documents:
· All records, emails and communications related to the participation of NIST employees in the development of the (ANSI) X9.82 standard for Random Number Generation from the period 2002 through 2007.

· All records, emails and communications related to the participation of NIST employees in the development of NIST Special Publication 800-90, during the period 2002-2007.

Thank you for your attention to this matter. Please follow up with my Senior Policy Advisor, Matt Stoller (matt.stoller@mail.house.gov or 202-225-9889).

Sincerely,

Alan Grayson
Member of Congress