November 28, 2007

Dear Bruce,

In your November 14, 2007 Wired commentary (http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115), you suggested that the Dual_EC_DRBG random number generator published in NIST Special Publication 800-90 has a property "that can only be described as a back door." We have no evidence that anyone has, or will ever have, the "secret numbers" for the back door that were hypothesized by mathematicians Dan Shumow and Neils Ferguson, that would provide advance information on the random numbers generated by the algorithm. For this reason, we are not withdrawing the algorithm at this time. NIST Special Publication 800-90, which includes a method for randomly generating points if there is a concern about a back door, underwent a rigorous review process that included a public comment period before it was published,. All NIST algorithms, including the Dual_EC_DRBG, undergo continual review throughout their lifetime. If successful attacks are found on an algorithm, the algorithm is withdrawn.

Sincerely,

Elaine Barker
Lead Author, NIST SP 800-90
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD