IS “BRIBERY” A DEMAND, OR A POLITE REQUEST?

Back when the NSA sent its employees home with a claim that said,

> NSA does not and will not demand changes by any vendor to any product, nor does it have any authority to demand such changes.

I said,

> Again, watch the language carefully. NSA denies it demands changes (presumably meaning to the security of software and hardware producers). It doesn’t deny it sometimes asks for changes. It doesn’t deny it sometimes negotiates unfairly to get those changes. It doesn’t deny it steals data on those changes.
>
> It just doesn’t demand those changes.

The NSA Review Group used almost precisely the same formulation in its non-denial denial that NSA corrupts encryption.

> NSA will not demand changes in any product by any vendor for the purpose of undermining the security or integrity of the product, or to ease NSA’s clandestine collection of information by users of the product;

Yesterday, Reuters explained how computer security firm, RSA, came to use the encryption standard, Dual_EC_DRBG, the NSA corrupted.

> Documents leaked by former NSA contractor Edward Snowden show that the NSA created and promulgated a flawed formula for generating random numbers to create a “back door” in encryption

> products, the New York Times reported in September. Reuters later reported that RSA became the most important distributor of that formula by rolling it into a software tool called Bsafe that is used to enhance security in personal computers and many other products.
>
> Undisclosed until now was that RSA received $10 million in a deal that set the NSA formula as the preferred, or default, method for number generation in the BSafe software, according to two sources familiar with the contract. Although that sum might seem paltry, it represented more than a third of the revenue that the relevant division at RSA had taken in during the entire previous year, securities filings show.

So I guess NSA considers “provide a third of a division’s revenue” a polite request, not a demand.

That’s not all that surprising. Before we’re done with this scandal, I expect we’ll learn the NSA is getting all sorts of cooperation via strong-armed cooperation. For example, we have reason to believe the NSA is relying on telecoms “voluntarily” providing “foreign” telecom communications. And there are a lot of tech and software companies that have divisions with falling revenues.

Remember — as William Ockham noted and security prof Matthew Green has emphasized on Twitter — this standard doesn’t appear in the Appendix the Review Group used to support their claim that “Upon review, however, we are unaware of any vulnerability created by the US Government in generally available commercial software that puts users at risk of criminal hackers or foreign governments decrypting their data,” the statement which appears just before they say they don’t “demand” these changes.

Which is yet further proof that that section of the Report was meant to minimize corporate risk, not end-user risk.