THE NSA REVIEW GROUP'S NON-DENIAL DENIAL ON ENCRYPTION

As part of a section on "Technical Measures to Increase Security and User Confidence," Recommendation 29 of the NSA Review Group is, in part, the following:

> We recommend that, regarding encryption, the US Government should:
>
> (1) fully support and not undermine efforts to create encryption standards;
>
> (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software;

Several paragraphs into this section, the Group with no tech experts asserts,

> 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. Moreover, it appears that in the vast majority of generally used, commercially available encryption software, there is no vulnerability, or "backdoor," that makes it possible for the US Government or anyone else to achieve unauthorized access.

This appears to be based on an Appendix provided by NSA addressing the reliability of certain encryption systems. I'm not competent to assess the claims or comprehensiveness of that presentation and eagerly await some reviews of this report from the tech experts. [Update: William Ockham notes the Appendix doesn't include the standard NSA is accused of weakening.]

The very next paragraph, with bullet points, reads,

> Nonetheless, it is important to take strong steps to enhance trust in this basic underpinning of information technology. Recommendation 32 is designed to describe those steps. The central point is that trust in encryption standards, and in the resulting software, must be maintained. Although NSA has made clear that it has not and is not now doing the activities listed below, the US Government should make it clear that:
>
> - *NSA will not engineer vulnerabilities into the encryption algorithms that guard global commerce;*
> - *The United States will not provide competitive advantage to US firms by the provision to those corporations of industrial espionage;*
> - *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; and*
> - *NSA will not hold encrypted communication*

> *as a way to avoid retention limits.*

I consider myself a bit of an aficionado in NSA claims, and I can only think of one place where they've made even some of these claims, sort of: the obviously bogus talking points NSA sent home at Thanksgiving. That document made a similar caveated comment about industrial espionage and assured that NSA will not demand changes by any vendor, noting it did not have the authority to do so. I pointed out some of the loopholes to those claims here.

I don't think they have said anything about engineering vulnerabilities into encryption standards; in any case, the allegation was that they inserted vulnerabilities into certain standards through persuasion, not engineering. Besides, ODNI General Counsel Robert Litt has stated explicitly (and not all that surprisingly) that cracking encryption is their job.

Finally, I don't think the NSA has ever addressed the fact that their minimization standards clearly allow them to keep encrypted communication forever. They like to lie about that one instead. To place in their mouth a claim that they won't do so to get around retention limits (particularly followed, as it is, by a recommendation for how not to do this) is thin comfort coming from an agency that considers encryption possible evidence of terrorism.

I doubt this assertion that NSA doesn't try to weaken encryption is fooling anyone. Indeed, it appears less than 30 pages after the Report states, in justifying moving Information Assurance out of NSA,

> When the offensive personnel find some way into a communications device, software system, or network, they may be reluctant to have a patch that blocks their own access.

So it's hard to treat this entire passage as anything else but the "strong step to enhance trust" they say is necessary within it.

The NSA Review Group makes worthwhile recommendations on a reorganization of NSA—the most aggressive one of which — to split the DIRNSA from the CyberCommand position — Obama already pre-empted. Moving Information Assurance out of NSA would also create a champion for privacy, albeit a hopelessly weak one (they even state it should be moved to DHS, but Congress would never agree to do so).

But ultimately on this and some other cybersecurity related issues (including its toothless recommendation on Zero Days that immediately follows this section), the Report serves only to pretend the US doesn't engage in weakening security as part of its offensive attacks using the Internet.

Update: Oh, as to that Appendix that doesn't include the standard everyone has been worried about? Someone's just found a fatal bug in the standard.

> An advisory published Thursday warns that a "FIPS module" of the widely used OpenSSL library contained a "fatal bug" in its implementation of Dual EC_DRBG. Credible doubts about the trustworthiness of the deterministic random bit generator surfaced almost immediately after National Security Agency (NSA) officials shepherded it through an international standards body in 2006. In September, those fears were rekindled when *The New York Times* reported the algorithm may contain an NSA-engineered backdoor that makes it easier for government spies to decode encrypted communications.
>
> The fatal Dual EC_DRBG bug resides in the FIPS Object Module v2.0, an optional OpenSSL library used to build crypto apps that are certified by the US

> government's Federal Information Processing Standards. When using the module's implementation of Dual EC_DRBG, the application crashes and can't be recovered. That's an amazing discovery for an application that had to undergo countless hours of testing to be certified by the government of the world's most powerful country.