

NOT BREAKING: KEITH ALEXANDER TO BE ALLOWED TO RETIRE UNSCATHED; BREAKING: NSA

We've actually known for some time that Keith Alexander was retiring shortly. So Reuters' headline reporting it (and the departure of Alexander's Deputy John Inglis) is not news.

U.S. eavesdropping agency chief, top deputy expected to depart soon

But mega kudos to the person who dubbed Alexander the "eavesdropping agency chief."

One important implication of this headline though is,

**Alexander will
not be fired,
much less
criminally
charged, for
serial lies to
Congress**

Not to mention the fact that James Clapper will, as far as we know, remain employed and free.

All that said, the overall point of Reuters' story is important. This presents Obama with an

opportunity to set a new direction for NSA.

While both men are leaving voluntarily, the dual vacancies give Obama an opportunity both to install new leadership following Snowden's revelations and to decide whether the NSA and Cyber Command should have separate leaders.

Cyber Command, which has grown significantly in recent years, has the authority to engage in both defensive and offensive operations in cyberspace. Many NSA veterans argue that having the same person lead the spy agency and Cyber Command diminishes the emphasis on the NSA's work and its unique capabilities.

I say go even bigger than this: break up this Frankenstein contraption and split NSA's defensive function from its offensive ones entirely. And while we're at it, let's move it out of DOD.

Noah Shachtman wrote a piece describing how to do this so long ago he actually referred to "the agency that tapped AT&T switching stations (OK, OK, allegedly)" instead of "the agency FISC deemed in violation of the Fourth Amendment for collecting US person data at AT&T's switches."

NSA headquarters – the "Puzzle Palace" – in Fort Meade, Maryland, is actually home to two different agencies under one roof. There's the signals-intelligence directorate, the Big Brothers who, it is said, can tap into any electronic communication. And there's the information-assurance directorate, the cybersecurity nerds who make sure our government's computers and telecommunications systems are hacker- and eavesdropper-free. In other words, there's a locked-down spy division and a relatively open geek division. The

problem is, their goals are often in opposition. One team wants to exploit software holes; the other wants to repair them.

[snip]

A broken-out bureau – call it the Cyber Security Agency, or CSA – that didn't include the spooks would obviate this conflict. "A separate information-assurance agency," says Michael Tanji, a 21-year veteran of intelligence services, including the NSA, "will have a greater level of acceptance across the government and the private sector."

[snip]

An independent CSA would be trusted more widely than Fort Meade, improving collaboration among cybersecurity geniuses. It was private researchers and academics who led the effort to corral the ultrasophisticated Conficker worm. And the National Institute of Standards and Technology worked on federal desktop security. A well-run, independent CSA would be able to coordinate better with these outside entities.

The problem – both of NSA's conflicting missions and of the lack of trust in it – has gotten far worse since Shachtman wrote this piece. The NYT reported that the NSA has been ensuring it has back doors in far more places than originally thought. In addition there are the concerns about its use of NIST to weaken encryption standards.

And we now know that NSA is keeping encrypted communications – including that of the white hats you need to cooperate on the cyberdefense project – indefinitely. That is, it is treating necessary partners as criminals.

Right now, the NSA wants to be able to copy and scan all the traffic in the US to be able to

search for malware and other malicious code. Yet it has already been caught spying on Americans even while just (allegedly) hunting for terrorists. And it refuses to count how many Americans it has spied on in this way. This is not a trustworthy agency to conduct out whatever sorting that needs to be done (not to mention the fact it can't be trusted to keep this goal separate from its offensive ones).

Even NSA's apologists should embrace such a suggestion. Without it, their claims to want the best defense against cyberthreats ring hollow, because the existing NSA is one of the biggest cyberdangers out there.