AS WITH MANNING LEAK, SNOWDEN LEAK REVEALS DOD DOESN'T PROTECT SECURITY

MSNBC has an update to the continuing saga of "Omigod the NSA has inadequate security." It explains why the "thin client" system the NSA had (one source calls it 2003 technology) made it so easy for Edward Snowden to take what he wanted.

> In a "thin client" system, each remote computer is essentially a glorified monitor, with most of the computing power in the central server. The individual computers tend to be assigned to specific individuals, and access for most users can be limited to specific types of files based on a user profile.
>
> But Snowden was not most users.
>
> [snip]
>
> As a system administrator, Snowden was allowed to look at any file he wanted, and his actions were largely unaudited. "At certain levels, *you are* the audit," said an intelligence official.
>
> He was also able to access NSAnet, the agency's intranet, without leaving any signature, said a person briefed on the postmortem of Snowden's theft. He was essentially a "ghost user," said the source, making it difficult to trace when he signed on or what files he accessed.
>
> If he wanted, he would even have been able to pose as any other user with access to NSAnet, said the source.

The story goes on to note that being in Hawaii would have allowed Snowden to access Fort Meade’s computers well after most users were gone.

I’m particularly interested in the assertion that Snowden could pose as any other user with access to NSAnet.

Any other user. Presumably, that includes at least Cybercommander Keith Alexander’s aides.

In a world in which the NSA is increasingly an offensive organization, certain figures within NSA would be engaged in some very interesting communications and compartments, I’d imagine.

Ah well. The US won’t learn. They’ll continue to neglect these holes until someone publicly demonstrates their negligence, all the while leaving them open for whatever paid agents of foreign governments choose to exploit them.