INTELLIGENCE COMMUNITY WILL CLOSE GAPING HOLE THAT ALLEGEDLY LED TO WIKILEAKS DISCLOSURE … IN 2013

I did a long post yesterday describing how embarrassingly, pathetically bad DOD's information security was and remains 3 years after a malware attack and a full year after the alleged WikiLeaks leak. Along with DOD's gaping security problems, I noted that some entities in the intelligence community are still in the process of implementing user authentication which would have exposed someone taking entire databases off of their networks.

> While the two DIA witnesses mostly blew smoke rather than provide a real sense of where security is at (both blamed WikiLeaks on a "bad apple" rather than shockingly bad information security), the testimony of DNI's Intelligence Community Intelligence Sharing Executive Corin Stone seems to suggest other parts of the IC area also still implementing the kind of authentication most medium sized corporations employ.
>
> > To enable strong network authentication and ensure that networks and systems can authoritatively identify who is accessing classified information, the IC CIO is implementing user authentication technologies and is working with the IC elements to achieve certificate issuance to eligible IC personnel in the first quarter of fiscal year 2012.

Just in case the intelligence community can't get around to providing this fairly common security on our intelligence community networks by their planned timeframe of the first quarter of FY 2012 (which would mean the last quarter of calendar year 2011), the Senate Intelligence Committee is requiring the IC to have a fully operational ability to audit online access by October 2013.

> Section 402 requires the Director of National Intelligence, not later than October 1, 2012, to establish an initial operating capability for an effective automated insider threat detection program for the information resources in each element of the Intelligence Community in order to detect unauthorized access to, or use or transmission of, classified information. Section 402 requires that the program be at full operating capability by October 1, 2013.
>
> Not later than December 1, 2011, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the resources required to implement the program and any other issues the Director considers appropriate to include in the report.

In other words, if closing this security gap a year and a half after the leaks are alleged to have occurred is too tough, then they can go ahead and take another year or so to close the barn door.

Though to be fair, this deadline may come directly from the lackadaisical DOD, as the deadlines given here seem to match those DOD aspires to hit.

Now, maybe it's considered unpatriotic to note that our intelligence community—and its congressional overseers—are tolerating pretty shoddy levels of security all while insisting

that they takes leaks seriously.

But seriously: if our government is going to claim that leaks are as urgent as it does, if it’s going to continue to pretend that secrets are, you know, really secret, then it really ought to at least pretend to show urgency on responding to the gaping technical issues that will not only protect against leakers, but also provide better cybersecurity and protect against spies. Aspiring to fix those issues years after the fact really doesn’t cut it.