LIKE SSCI, HPSCI REQUIRES DNI TO CLOSE GAPING SECURITY HOLES … BY 2013

Steven Aftergood has the House intelligence report online and—as he points out—it contains a requirement that the intelligence community close one of the gaping holes in network security highlighted by the WikiLeaks case. The deadline? 2013.

> SEC. 402. INSIDER THREAT DETECTION PROGRAM.
>
> (a) Initial Operating Capability.—Not later than October 1, 2012, the Director of National Intelligence shall 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 intelligence.
>
> (b) Full Operating Capability.—Not later than October 1, 2013, the Director of National Intelligence shall ensure the program described in subsection (a) has reached full operating capability.
>
> (c) Report.—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 insider threat detection program referred to in subsection (a) and any other issues related to such implementation the Director considers appropriate to include in the report.
>
> (d) Information Resources Defined.—In

> this section, the term “information resources” means networks, systems, workstations, servers, routers, applications, databases, websites, online collaboration environments, and any other information resources in an element of the intelligence community designated by the Director of National Intelligence.

This is precisely what the Senate Intelligence Committee is also mandating. As I pointed out earlier, this seems to simply take DOD’s own lackadaisical deadline and make it a requirement.

> 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.

Ah well! Bin Laden is dead. Who else might want our secrets?