OBAMA ADMINISTRATION: SORRY, 2013 IS TOO SOON TO FIX GAPING HOLES IN OUR NETWORK SECURITY

You've no doubt read the multiple posts in which I responded with growing incredulity at the response of DOD and the Intelligence Community to the gaping holes in their network security.

Basically, a review of DOD networks after Bradley Manning's alleged leaking (which came two years after they reviewed DOD networks after a bad malware infection introduced via a thumb drive), DOD admitted that they still let service members access computers on DOD's classified network with removable media (like Lady Gaga CDs) two years after they vowed to end the practice; they didn't have personal keys to offer better authentication and tracking of actions taken online; and they couldn't audit for unusual activities online.

In short, they don't have the kind of security that is considered routine in the private sector.

On our classified network.

And in response to their admission of gaping holes in Department of Defense's (and presumably, because they want the same deadline, other parts of the IC's) network security, they laid out a plan to fix the problems … by 2013.

Cause I'm sure none of our enemies will come looking for our secrets between now and then.

It's becoming an obsession for me, this disinterest in fixing gaping holes in our network security even as the Administration claims Bradley Manning's alleged leak could be a

capital offense. If this stuff is so damned secret, plug the fucking holes!

So you can imagine my shock when I read the Obama Administration's response to the intelligence bill's endorsement of the 2013 deadline DOD and the IC asked for: (h/t Steven Aftergood)

> Section 402 requires the DNI to create an insider threat detection program for the information resources of each element of the IC to detect unauthorized access to classified information. The Administration wholeheartedly agrees with the need to be vigilant and proactive in trying to detect, mitigate, and deter insider threats, and supports a comprehensive insider threat detection capability. The Administration is currently working toward its implementation. However, the Administration is concerned with the unrealistic timelines required by this provision for the program's operational readiness, and strongly requests that the provision be amended to grant the DNI flexibility in implementation timelines of the program.

Hey bad guys?!?!?!? No one is checking the intelligence community's networks to see whether you're nicking highly classified information off of them. No one is checking their networks to see what kind of abnormal activities their own spooks are engaging in.

And they're not going to be until … well, they don't know. A deadline, you see, would be rather restrictive. And our fucking classified networks just aren't a priority for network security! All I can tell you is 2013—two full years from now—that's too soon.

So China, Iran? Just take what you want. Just make sure you do it in the next two … or maybe three … or who knows? years, because sometime in

the distant future the IC aspires to have the same kind of network security your average bland business has.