AND SINCE WE'VE BEEN TALKING ABOUT CONTRACTING, SECRECY, AND SPYING…

…In our discussion of Tim Shorrock's *Spies for Hire*, it seems appropriate to post on the Senate Armed Services Committee's report on the Cyber-Security Initiative.

As you'll recall, the Bush Administration has been struggling for their entire term to address the fact that our cyber-infrastructure is woefully exposed to cyber-attacks. After a series of cyber-czars who either wouldn't or couldn't address this problem, back in January the Administration began to make some progress—not least, by taking the project out of Michael Chertoff's hands. The SASC's report notes that the Administration has made some progress, though it has three substantive complaints.

> The committee applauds the administration for developing a serious, major initiative to begin to close the vulnerabilities in the government's information networks and the nation's critical infrastructure. The committee believes that the administration's actions provide a foundation on which the next president can build.
>
> However, the committee has multiple, significant issues with the administration's specific proposals and with the overall approach to gaining congressional support for the initiative.

First, the SASC objects to the way the Administration has shielded what is supposed to be at least partly a deterrent program in so much secrecy that the program has lost its

deterrence ability.

> A chief concern is that virtually everything about the initiative is highly classified, and most of the information that is not classified is categorized as `For Official Use Only.' These restrictions preclude public education, awareness, and debate about the policy and legal issues, real or imagined, that the initiative poses in the areas of privacy and civil liberties. Without such debate and awareness in such important and sensitive areas, it is likely that the initiative will make slow or modest progress. The committee strongly urges the administration to reconsider the necessity and wisdom of the blanket, indiscriminate classification levels established for the initiative.
>
> The administration itself is starting a serious effort as part of the initiative to develop an information warfare deterrence strategy and declaratory doctrine, much as the superpowers did during the Cold War for nuclear conflict. **It is difficult to conceive how the United States could promulgate a meaningful deterrence doctrine if every aspect of our capabilities and operational concepts is classified**. In the era of superpower nuclear competition, while neither side disclosed weapons designs, everyone understood the effects of nuclear weapons, how they would be delivered, and the circumstances under which they would be used. **Indeed, deterrence was not possible without letting friends and adversaries alike know what capabilities we possessed and the price that adversaries would pay in a real conflict**. Some analogous level of disclosure is necessary in the cyber domain.

Not only can't citizens debate aspects of the program with so much secrecy, but we also can't tell the Chinese hackers who would like to shut our systems down what will happen if they try to do so. (Hmm, I wonder if the worry is that the Chinese hackers wouldn't be too concerned?) For more on this complaint, see Steven Aftergood.

To add to the concerns that secrecy prevents any meaningful debate, SASC notes, the initiative is moving far ahead of standard requirements for acquisitions: the Administration is trying to get Congress to pay for stuff that just isn't ready yet.

> The committee also shares the view of the Senate Select Committee on Intelligence that major elements of the cyber initiative request should be scaled back because policy and legal reviews are not complete, and because the technology is not mature. Indeed, the administration is asking for substantial funds under the cyber initiative for fielding capabilities based on ongoing programs that remain in the prototype, or concept development, phase of the acquisition process. These elements of the cyber initiative, in other words, could not gain approval within the executive branch if held to standards enforced on normal acquisition programs. The committee's view is that disciplined acquisition processes and practices must be applied to the government-wide cyber initiative as much as to the ongoing development programs upon which the initiative is based.

Hmm. The Committee seems right to be worried that the Administration wants us taxpayers to pay for "concepts" in secret.

And then, there's the issue that Ryan Singel hits on—the Administration is trying to get us to pay for stuff, in the name of Cyber-Security, that is really just more spying.

> The committee also concludes that some major elements of the cyber initiative are not solely or even primarily intended to support the cyber security mission. Instead, it would be more accurate to say that some of the projects support foreign intelligence collection and analysis generally rather than the cyber security mission particularly. If these elements were properly defined, the President's cyber security initiative would be seen as substantially more modest than it now appears. That is not to say that the proposed projects are not worthwhile, but rather that what will be achieved for the more than $17.0 billion planned by the administration to secure the government's networks is less than what might be expected.

The Administration is waving a $17 billion price tag around, which won't get us the Cyber-Security the project is intended to, but will get us a bunch of other spying programs that really aren't about Cyber-Security. No word, then, on what the real price tag would end up being to actually implement a Cyber-Security program that, you know, is something more than a concept. $17 billion is an awful lot for a concept with some more spying added in just for kicks.

Finally, the SASC attaches a laundry list of other major problems with the program—which basically make it sound like this isn't a "program" yet at all.

> Finally, the committee concludes that, for all its ambitions, the cyber initiative sidesteps some of the most important issues that must be addressed to develop the means to defend the country. These tough issues include the establishment of clear command chains, definition of roles and missions for the various agencies and departments, and

> engagement of the private sector.

Though, given the discussion we had earlier today, it sure seems like the Intelligence Community really hasn't yet figured out the chain of command, defined the roles and missions, and figured out how to integrate the private sector effectively anyway.

All in all, this report looks like the kind of report you'd get from a very positive elementary school teacher. "Very nice try, Johnny. It's so nice to see you trying to finish the homework you've been working on for eight years. Now let's talk about the bare minimum you're going to need to do in order to actually complete this homework. And no, you can't have $17 billion dollars for what thus far is still C minus work."