THREE CONGRESSIONAL RESPONSES TO THE OPM HACK

After acknowledging that as more than 20 million people have been affected by the hack of the Office of Personnel Management, OPM head Katherine Archuleta "resigned" today.

In announcing that Office of Budget and Management Deputy Director of Management Beth Cobert would serve as acting Director, Josh Earnest played up her experience at McKinsey Consulting. So we may see the same kind of management claptrap as OPM PR in the coming days that we got from CIA's reorganization when McKinsey took that project on. Over 20 minutes into his press conference, Earnest also revealed there was 90 day review of the security implications of the hack being led by OMB.

Happily, in spite of the easy way Archuleta's firing has served as a proxy for real solutions to the government's insecurity, at least some in Congress are pushing other "solutions." Given Congress' responsibility for failing to fund better IT purchasing, consider agency weaknesses during confirmation, and demand accountability from the intelligence community going back at least to the WikiLeaks leaks, these are worth examining.

Perhaps most predictably, Susan Collins called for passage of cybersecurity legislation.

> It is time for Congress to pass a cybersecurity law that will strengthen our defenses and improve critical communication and cooperation between the private sector and government. We must do more to combat these dangerous threats in both government and the private sector.

Of course, nothing in CISA (or any other

cybersecurity legislation being debated by Congress) would have done a damn thing to prevent the OPM hack. In other words, Collins' response is just an example of Congress doing the wrong thing in response to a real need.

Giving corporations immunity is not the answer to most problems facing this country. And those who embrace it as a real solution should be held accountable for the next government hack.

Freshman Nebraska Senator Ben Sasse — both before and after Archuleta's resignation — has appropriately laid out the implications of this hack (rebutting a comparison repeated by Earnest in his press conference, that this hack compares at all with the Target hack).

> OPM's announcement today gives the impression that these breaches are just like some of the losses by Target or Home Depot that we've seen in the news. The analogy is nonsense. This is quite different—this is much scarier than identity theft or ruined credit scores. Government and industry need to understand this and be ready. That's not going to happen as long as Washington keeps treating this like just another routine PR crisis.

But one of his proposed responses is to turn this example of intelligence collection targeting legitimate targets into an act of war.

> Some in the defense and intelligence communities think the attacks on OPM constitute an act of war. The rules of engagement in cyber warfare are still being written. And with them, we need to send a clear message: these types of intrusions will not be tolerated. We must ensure our attackers suffer the full consequences of their actions.
>
> Starting now, government needs to stop the bleeding—every sensitive database in every government agency must be

> immediately secured or pulled offline. But playing defense is a losing game. Naming and shaming until the news cycle shifts is not enough.
>
> Our government must completely reevaluate its cyber doctrine. We have to deter attacks from ever happening in the first place while also building resiliency.

We're collecting the same kind of information as China — in methods that are both more efficient (because we have the luxury of being able to take off the Internet) but less so (because we are not, as far as we know, targeting China's own records of its spooks). If this is an act of war than we gave reason for war well before China got into OPM's servers.

Meanwhile, veterans Ted Lieu and Steve Russell (who, because they've had clearance, probably have been affected) are pushing reforms that will affect the kind of bureaucracy we should have to perform what is a core counterintelligence function.

> Congressman Russell's statement:
>
> "It is bad enough that the dereliction displayed by OPM led to 25 million Americans' records being compromised, but to continue to deflect responsibility and accountability is sad. In her testimony a few weeks ago, OPM Director Katherine Archuleta said that they did not encrypt their files for fear they could be decrypted. This is no excuse for a cyber-breach, and is akin to gross negligence. We have spent over a half a trillion dollars in information technology, and are effectively throwing it all away when we do not protect our assets. OPM has proven they are not up to the task of safeguarding our information, a responsibility that allows for no error.

> I look forward to working with Congressman Lieu on accountability and reform of this grave problem."
>
> Congressman Lieu's statement:
>
> "The failure by the Office of Personnel Management to prevent hackers from stealing security clearance forms containing the most private information of 25 million Americans significantly imperils our national security. Tragically, this cyber breach was likely preventable. The Inspector General identified multiple vulnerabilities in OPM's security clearance system—year after year—that OPM failed to address. Even now, OPM still does not prioritize cybersecurity. The IG testified just yesterday that OPM 'has not historically, and still does not, prioritize IT security.' The IG further testified that there is a 'high risk' of failure on a going forward basis at OPM. The security clearance system was previously housed at the Department of Defense. In hindsight, it was a mistake to move the security clearance system to OPM in 2004. We need to correct that mistake. Congressman Steve Russell and I are working on bipartisan legislation to move the security clearance database out of OPM into another agency that has a better grasp of cyber threats. Steve and I have previously submitted SF-86 security clearance forms. We personally understand the national security crisis this cyber breach has caused. Every American affected by the OPM security clearance breach deserves and demands a new way forward in protecting their most private information and advancing the vital security interests of the United States."

A number of people online have suggested that seeing Archuleta get ousted (whether she was

forced or recognized she had lost Obama's support) will lead other agency heads to take cybersecurity more seriously. I'm skeptical. In part, because some of the other key agencies — starting with DHS — have far to much work to do before the inevitable will happen and they'll be hacked. But in part because the other agencies involved have long had impunity in the face of gross cyberintelligence inadequacies. No one at DOD or State got held responsible for Chelsea Manning's leaks (even though they came 2 years after DOD had prohibited removable media on DOD computers), nor did anyone at DOD get held responsible for Edward Snowden's leaks (which happened 5 years after the ban on removable media). Neither the President nor Congress has done anything but extend deadlines for these agencies to address CI vulnerabilities.

Perhaps this 90 day review of the NatSec implications of the hack is doing real work (though I worry it'll produce McKinsey slop). But this hack should be treated with the kind of seriousness as the 9/11 attack, with the consequent attention on real cybersecurity fixes, not the "do something" effort to give corporations immunity.