WHY IS DEVIN NUNES RUSHING TO GIVE MORE DATA TO HACK-TASTIC DEPARTMENT OF ENERGY?

On several occasions, I've pointed out that the agencies that would automatically receive data shared with the federal government under cybersecurity bills being pushed through Congress aren't any more secure than Office of Personnel Management, which China hacked in spectacular fashion. Among the worst – and getting worse rather than better – is Department of Energy.

Earlier this week, USAT published more information on how bad things are at DoE.

> Cyber attackers successfully compromised the security of U.S. Department of Energy computer systems more than 150 times between 2010 and 2014, according to a review of federal records obtained by USA TODAY.
>
> Incident reports submitted by federal officials and contractors since late 2010 to the Energy Department's Joint Cybersecurity Coordination Center shows a near-consistent barrage of attempts to breach the security of critical information systems that contain sensitive data about the nation's power grid, nuclear weapons stockpile and energy labs.
>
> The records, obtained by USA TODAY through the Freedom of Information Act, show DOE components reported a total of 1,131 cyberattacks over a 48-month period ending in October 2014. Of those attempted cyber intrusions, 159 were successful.

Yet at yesterday's Cyber Threats hearing (around 2 minutes), House Intelligence Chair Devin Nunes suggested he only learned of this detail from USAT's report. "[J]ust this morning we learned that Department of Energy was successfully hacked 159 times."

It's troubling enough that the guy overseeing much of the government's cybersecurity efforts didn't already know these details (and I presume that means Nunes is also unaware that DoE has actually been getting *worse* as the Administration tries to fix major holes). Especially given that DoE is part of the Intelligence Community.

But it's even more troubling given that HPSCI's Protecting Cyber Networks Act, like the Senate's Cyber Intelligence Sharing Act, automatically shares incoming cyber threat data with DoE (and permits private entities to share with DoE directly).

This is the height of irresponsibility. Devin Nunes is rushing to share this data — he pushed for quick passage of these bills in the same breath as noting how insecure DoE is —yet he hadn't even bothered to review whether the agencies that would get the data have a consistent history of getting pawned.

Nunes did say that we need to ensure these agencies are secure. But the data is clear: DoE *isn't* secure.

So why not plug those holes before putting more data in for hackers to get?