CISA HACK OF THE DAY: WHITE HOUSE CAN ALREADY SHARE INTELLIGENCE WITH THE STATE DEPARTMENT

In about 10 days, Congress will take up cyber information sharing bills. And unlike past attempts, these bills are likely to pass.

That, in spite of the fact that no one has yet explained how they'll make a significant difference in preventing hacks.

So I'm going to try to examine roughly one hack a day that immunized swift information sharing between the government and the private sector wouldn't prevent.

Yesterday, for example, CNN reported that Russia had hacked "sensitive parts" (read, unclassified) of the White House email system.

> While the White House has said the breach only affected an unclassified system, that description belies the seriousness of the intrusion. The hackers had access to sensitive information such as real-time non-public details of the president's schedule. While such information is not classified, it is still highly sensitive and prized by foreign intelligence agencies, U.S. officials say.
>
> The White House in October said it noticed suspicious activity in the unclassified network that serves the executive office of the president. The system has been shut down periodically to allow for security upgrades.
>
> The FBI, Secret Service and U.S. intelligence agencies are all involved in investigating the breach, which they

> consider among the most sophisticated attacks ever launched against U.S. government systems. The intrusion was routed through computers around the world, as hackers often do to hide their tracks, but investigators found tell-tale codes and other markers that they believe point to hackers working for the Russian government.

The hackers – whether they really are Russian government operatives or not – managed the hack by first hacking the State Department and then phishing an account at the White House using a State email.

> To get to the White House, the hackers first broke into the State Department, investigators believe.
>
> The State Department computer system has been bedeviled by signs that despite efforts to lock them out, the Russian hackers have been able to reenter the system. One official says the Russian hackers have "owned" the State Department system for months and it is not clear the hackers have been fully eradicated from the system.
>
> As in many hacks, investigators believe the White House intrusion began with a phishing email that was launched using a State Department email account that the hackers had taken over, according to the U.S. officials.

In other words, the hackers breached the White House by first hacking State – a hack that was well known to the government – and then duping some schmoe at the White House to compromise their email.

Now, unless things have gone really haywire in the government, nothing prevents the State Department from sharing information with the White House. Indeed, NSA and DHS should have an

active role in both hacks. Nor would anything prevent NSA from sharing information on the proxy computers used by the hackers. And if NSA can't find those, we have other problems.

Finally, there's little a private company could tell the White House to get its schmoes to be a bit more cautious about the email they get (though I suspect in both State and the White House, it is hard to balance responsiveness with adequate skepticism to odd emails).

In other words, CISA would do nothing to prevent this hack of the White House. But nevertheless, Congress is going to rush through this bill without fixing other more basic vulnerabilities.