THE PRO-SCRUB LANGUAGE ADDED TO CISA IS DESIGNED TO ELIMINATE DHS' SCRUB

I've been comparing the Manager's Amendment (MA) Richard Burr and Dianne Feinstein introduced Wednesday with the old bill.

A key change — one Burr and Feinstein have highlighted in their comments on the floor — is the integration of DHS even more centrally in the process of the data intake process. Just as one example, the MA adds the Secretary of Homeland Security to the process of setting up the procedures about information sharing.

> Not later than 60 days after the date of the enactment of this Act, the Attorney General *and the Secretary of Homeland Security* shall, in coordination with the heads of the appropriate Federal entities, develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government. [my emphasis]

That change is applied throughout.

But there's one area where adding more DHS involvement appears to be just a show: where it permits DHS conduct a scrub of the data on intake (as Feinstein described, this was an attempt to integrate Tom Carper's and Chris Coons' amendments doing just that).

This is also an issue DHS raised in response to Al Franken's concerns about how CISA would affect their current intake procedure.

> To require sharing in "real time" and "not subject to any delay [or] modification" raises concerns relating to operational analysis and privacy.

> First, it is important for the NCCIC to be able to apply a privacy scrub to incoming data, to ensure that personally identifiable information unrelated to a cyber threat has not been included. If DHS distributes information that is not scrubbed for privacy concerns, DHS would fail to mitigate and in fact would contribute to the compromise of personally identifiable information by spreading it further. While DHS aims to conduct a privacy scrub quickly so that data can be shared in close to real time, the language as currently written would complicate efforts to do so. DHS needs to apply business rules, workflows and data labeling (potentially masking data depending on the receiver) to avoid this problem.
>
> Second, customers may receive more information than they are capable of handling, and are likely to receive large amounts of unnecessary information. If there is no layer of screening for accuracy, DHS' customers may receive large amounts of information with dubious value, and may not have the capability to meaningfully digest that information.
>
> While the current Cybersecurity Information Sharing Act recognizes the need for policies and procedures governing automatic information sharing, those policies and procedures would not effectively mitigate these issues if the requirement to share "not subject to any delay [or] modification" remains.
>
> To ensure automated information sharing works in practice, DHS recommends requiring cyber threat information received by DHS to be provided to other federal agencies in "as close to real time as practicable" and "in accordance with applicable policies and

> procedures."

Effectively, DHS explained that if it was required to share data in real time, it would be unable to scrub out unnecessary and potentially burdensome data, and suggested that the "real time" requirement be changed to "as close to real time as practicable."

But compare DHS's concerns with the actual language added to the description of the information-sharing portal (the new language is in italics).

> (3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—
>
> (A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104(c) through the real-time process described in subsection (c) of this section—
>
> (i) are shared in an automated manner with all of the appropriate Federal entities;
>
> (ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—
>
> *(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;*
>
> *(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and*

> *(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and*

This section permits one of the "appropriate Federal agencies" to veto such a scrub. Presumably, the language only exists in the bill because one of the "appropriate Federal agencies" has *already* vetoed the scrub. NSA (in the guise of "appropriate Federal agency" DOD) would be the one that would scare people, but such a veto would equally as likely to come from FBI (in the guise of "appropriate Federal agency" DOJ), and given Tom Cotton's efforts to send this data even more quickly to FBI, that's probably who vetoed it.

If you had any doubts the Intelligence Community is ordering up what it wants in this bill, the language permitting them a veto on privacy protections should alleviate you of those doubts.

On top of NSA and FBI's veto authority, there's an intentional logical problem here. DHS is one of the "appropriate Federal agencies," but DHS is the entity that would presumably do the scrub. Yet if it can't retain data before any other agency, it's not clear how it could do a scrub.

In short, this seems designed to lead people to believe there might be a scrub (or rather, that under CISA, DHS would continue to do the privacy scrub they are currently doing, though they are just beginning to do it automatically) when, for several reasons, that also seems to be ruled out by the bill. And ruled out because one "appropriate Federal agency" (like I said, I suspect FBI) plans to veto such a plan.

So it has taken this Manager's Amendment to explain why we need CISA: to make sure that DHS doesn't do the privacy scrubs it is currently doing.

I'll explain in a follow-up post why it would be

so important to eliminate DHS’ current scrub on incoming data.