# CAN (SHOULD?) DHS STAVE OFF CISA?

Yesterday, DHS Secretary Jeh Johnson announced some shifts in the leadership of the National Cybersecurity and Communications Integration Center. The changes don't amount to much — basically a change in reporting for Dr. Andy Ozment, who is already Assistant Secretary of the Office of Cybersecurity and Communications (though it's worth noting that Ozment is one of the too-rare people high level in government cybersecurity positions with a technical background). Now, Ozment will report directly to Johnson.

But I am interested in the way DHS is making news, and when.

Last week, Al Franken released the response from DHS he got to some inquiries, notably about how the Cyber Information Sharing Act would affect efforts already underway to share data. Most reporting on it focused on privacy — that's what Franken himself emphasized — but the letter itself provided far more detail on the information sharing already taking place through NCCIC.

The letter described five different means of sharing information currently in place.

- In-person information sharing on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor;
- Bilateral sharing of cyber threat indicators, including via the Cyber Information Sharing and Collaboration Program (CISCP) and through automated sharing and

receipt of cyber threat indicators;
- As-needed information sharing via standing groups;
- Broad dissemination of alerts and bulletins;
- Strategic engagement and collaboration.

I was rather curious about the agencies with which NCCIC currently shares data.

- US Northern Command
- US Cyber Command
- National Security Agency
- Secret Service
- Immigration and Customers Enforcement
- Department of the Treasury
- FBI
- Department of Energy

This is a different list than the agencies that would automatically receive data under CISA — Commerce (which appears to serve a carrot-and-stick force in such issues) and the Office of Director of National Intelligence would not be on the list.

DHS also claimed to be "beginning to share 'machine-readable' cyber threat indicators and notes it will be expanding how many partners it will do so later this year.

Finally, as I noted earlier, DHS said it would take 6 months to implement the information sharing portal envisioned by CISA in place.

All of which is to say that DHS made a bid with this letter to Franken to say (as I interpreted), "we're sharing data right now, but if CISA passes, not only will Americans get less protection, but it will stall cybersharing for 6 months."

And now DHS is increasing the profile of its cyber staff.

I'd say all that was just bureaucratic wrangling — and it is that.

Except I think there is an opportunity, given the recess, the increasing calls for more substantive cyber legislation, and the inevitable roadblock once the Senate returns (particularly if, as is happening thus far, Ted Cruz is doing reasonably well or even poorly in the GOP Clown Show and has the incentive to cause headaches for Mitch McConnell in hopes of electoral gain) to present this as information sharing that is already advanced well beyond what CISA would do, and in a way that accomplishes what it is supposed to without the big downsides of CISA. That's still an outside chance. But increasingly possible and — given how dumb CISA is — probably a better solution.