TOM COTTON DOES NOTHING AS OPM HACK EQUIVALENT HAPPENS IN PLAIN SIGHT

Both WaPo and MuskWatch have written about the declaration that former acting Chief of Staff to the then-Acting Social Security Commissioner, Tiffany Flick, submitted in a union lawsuit against the Social Security Agency on Friday. To support a bid for a Temporary Restraining Order arguing, in part, that the way DOGE has handled Social Security data exposes the unions' members to fraud, Flick described how DOGE boys were given rushed access to the most sensitive kind of Social Security data, including:

> The Enterprise Data Warehouse, which houses SSA's master files and includes extensive information about anyone with a social security number (including names, names of spouses and dependents, work history, financial and banking information, immigration or citizenship status, and marital status);
>
> The Numident file, which contains information about the assignment of social security numbers; and
>
> The Master Beneficiary Record and SSI Record files, which contain detailed information (including medical data) about anyone who applies for or receives Social Security or SSI benefits

While WaPo's Lisa Rein (who has been covering this particular takeover closely and was cited in the filing) ends her piece quoting Flick saying, "the risk of data leaking into the wrong hands is significant," neither Rein nor MuskWatch considers the full implications of this. (And to be fair, the union's lawsuit, which represents general government employees,

doesn't either.)

Though this complaint includes a FISMA component, meaning the unions are arguing, in part, that the government is violating its own cybersecurity rules, it does not and cannot make a national security argument: That treatment of the entire country's data in this fashion presents enormous national security risks.

As Flick describes, Elon's DOGE boys came into the Social Security Agency harboring and clinging to conspiracy theories about fraud, even when offered explanations to debunk them.

> 20. [snip] We proposed briefings to help Mr. Russo and Mr. Bobba understand the many measures the agency takes to help ensure the accuracy of benefit payments, including those measures that help ensure we are not paying benefits to deceased individuals. However, Mr. Russo seemed completely focused on questions from DOGE officials based on the general myth of supposed widespread Social Security fraud, rather than facts.
>
> [snip]
>
> 51. Additionally, even with only read access DOGE can, and has already, used SSA data to spread mis/disinformation about the amount of fraud in Social Security benefit programs. The agency can always do more to ensure accurate and timely benefits payments, and it continues to pursue improvements. However, fraud is rare, and the agency has numerous measures in place to detect and correct fraud.

Having nothing more than conspiracy theories, DOGE demanded — and got (partly by replacing the Commissioner with a staffer who had worked with DOGE in advance) — that Akash Bobba be granted access to virtually all of Social Security Agency's data, immediately. Bobba appears, with description of his access at GSA, in this Wired

profile. Bobba got access to that data via a telework option, meaning he was located with a bunch of other people not cleared into this data itself.

> 22. Throughout this time, Acting Commissioner King requested that Mr. Russo report to her, as the CIO normally would, but he consistently gave evasive answers about his work. It appeared to me that he was actually reporting to DOGE.
>
> 23. During the week of February 10, with daily pressure from Mr. Russo, the CIO's office tried to rapidly train Mr. Bobba to get him access to SSA data systems so he could work on a special project for Mr. Russo at DOGE's request and so that he could "audit" any of the work of SSA experts.
>
> 24. We worked to provide Mr. Bobba with the necessary information and information security training but had to do so in a truncated manner and outside normal processes.
>
> 25. Given that, I do not believe Mr. Bobba had a sufficient understanding of the sensitive nature of SSA data or the ways to ensure such data's confidentiality. These are complicated systems with complex policies governing very large programs, and it simply is not possible to become proficient within a matter of days.
>
> [snip]
>
> 28. [snip] I understood that Mr. Bobba was working off-site at OPM while he was analyzing the SSA data. I also understood that other, non-SSA people were with him and may have also had access to the protected information. My understanding is that Mr. Russo approved a telework agreement for Mr. Bobba (while at the same time directing CIO

> management to work onsite full-time) to allow him to work out of OPM. But our standard telework agreements state that employees need to work in a private location and should be careful to protect systems and data from unauthorized access. Mr. Bobba's work didn't seem to align with those requirements.
>
> [snip]
>
> 36. It was never entirely clear what systems Mr. Russo wanted Mr. Bobba to have access to, but Mr. Russo reportedly stated that Mr. Bobba needed access to "everything, including source code."
>
> [snip]
>
> 43. But the request to give Mr. Bobba full access to these databases without justifying the "need to know" this information was contrary to SSA's longstanding privacy protection policies and regulations, and none of these individuals could articulate why Mr. Bobba needed such expansive access. I also understood that Mr. Bobba would not view the data in a secure environment because he was living and working at the Office of Personnel Management around other DOGE, White House, and/or OPM employees.

Even if we could assume these DOGE boys — at least three of whom (Edward "Big Balls" Coristine, Branden Spikes, and Sam Corcos) have been shown to have suspect ties — have no other motive than to spin false claims of fraud, this would still be a massive security risk. But as Flick repeats over and over, these DOGE boys were always evasive about what they were really up to. And as she describes, these boys are working off site, without the kind of confidentiality protections that would apply within SSA.

By handling the data like this, they make it child's play for adversaries to help themselves as well.

It's not just that DOGE has found almost nothing while compromising the most sensitive datasets in government. It's also that the way they're doing so, driven in significant part by this haste, has made it exceedingly more likely someone *else* will compromise the data.

The risk is not just fraud (the harm laid out in the lawsuit). It's spying, on an even greater scale than China achieved with the OPM hack.

And the members of Congress who're supposed to oversee such issues have done nothing — at least nothing public.

I've included contact numbers for the Senate Intelligence Committee (which is the most likely to give a shit about possible compromise like this), as well as the Chair and Ranking members of other committees with jurisdiction. If one of them is your Member of Congress, call and ask why they're abdicating their duty to protect the country from obvious compromise.

Senate Intelligence Committee

GOP

Tom Cotton (202) 224-2353

Jim Risch (202) 224-2752

Susan Collins (202) 224-2523

John Cornyn (202) 224-2934

Jerry Moran (202) 224-6521

James Lankford (202) 224-5754

Mike Rounds (202) 224-5842

Todd Young (202) 224-5623

Ted Budd (202) 224-3154

Dems

Mark Warner (202) 224-2023

Ron Wyden (202) 224-5244

Martin Heinrich (202) 224-5521

Angus King (202) 224-5344

Michael Bennett (202) 224-5852

Kirsten Gillibrand (202) 224-4451

Jon Ossoff (202) 224-3521

Mark Kelly (202) 224-2235

Senate Homeland Security Committee

Rand Paul (202) 224-4343

Gary Peters (202) 224-6221

House Intelligence Committee

Rick Crawford (202) 225-4076

Jim Himes (202) 225-5541

House Homeland Security Committee

Mark Green (202) 225-2811

Bennie Thompson (202) 225-5876