TIME TO GET VERY CONCERNED ABOUT CISA GUTTING GOVERNMENTAL LEVERAGE ON CORPORATIONS OVER CYBER

Back in August, I wrote a post wondering whether the following clause in the Cyber Intelligence Sharing Act would provide a way for corporations to avoid any government action punishing them for their negligence on cybersecurity.

> (D) FEDERAL REGULATORY AUTHORITY.—
>
> (i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this Act shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.
>
> (ii) EXCEPTIONS.—
>
> (I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this Act may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating

> to such information systems.
>
> (II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS ACT.—Clause (i) shall not apply to procedures developed and implemented under this Act.

My worry was that a serial hacking target like Wyndam — or even just a company with sloppy security like GM — could immediately share information on a hack (or even a vulnerability identified by security researcher that technically violated a company's DMCA rights) with the government, and in doing so avoid any further action from the government on that point.

Something similar appears to happen with the Bank Secrecy Act: banks share information and therefore limit their liability for money laundering or supporting terrorists or what have you.

If my concern is correct, it would provide companies that chose not to fix vulnerabilities a way to avoid NHTSA required recalls or FTC lawsuits.

At Computers Freedom and Privacy, I asked the author of CISA, Senate Intelligence staffer Josh Alexander, about the clause.

His only response was to point to this language permitting disclosure of information.

> (a) Otherwise Lawful Disclosures.—Nothing in this Act shall be construed—
>
> (1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by an entity to any other entity or the Federal Government under this Act; or
>
> (2) to limit or prohibit otherwise lawful use of such disclosures by any

> Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this Act.

He emphasized that the government could still respond to unlawful activity. But bad security is not unlawful.

In other words, he had no response to my concerns. Which leads me to believe CISA guts the government's ability to punish companies that don't fix their security issues.

I guess that explains why the Chamber of Commerce is so excited about the bill.