# WORKING THREAD, CYBERSECURITY ACT

As I've been reporting, Paul Ryan added a version of the Cybersecurity Information Sharing Act to the omnibus. It starts on page 1728. This will be my working thread.

(1745) They've changed what gets stripped from "person" to "individual," thereby not requiring that corporate names get stripped.

(1747) The bill takes out CISA's requirement of getting authorization before using an indicator for law enforcement.

(1753) The language on ensuring there are audit capabilities (but not that they're used) takes out this language, which was in CISA.

> C) consistent with this title, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled "National Strategy for Trusted Identities in Cyberspace" and published by the President in April, 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this title, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(1754) This section replaced an "or" in CISA with the underlined "and," which I think sharply constrains the list of stuff that shouldn't be shared. (It also replaces "person" with "individual" as consistent with other changes.)

> (i) Identification of types of information that would qualify as a cyber threat indicator under this title that would be unlikely to include information that—

> (I) is not directly related to a cybersecurity threat; and
>
> (II) is personal information of a specific individual or information that identifies a specific individual.

(1755) OmnibusCISA requires the AG to make both the interim and final privacy guidelines public; CISA had only made interim ones public.

> jointly issue and make publicly available final guidelines

(1760) The clause noting that other info sharing is still permissible adds the underlined language.

> (i) reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or a Federal entity, including cyber threat indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation;

(1761-2) The bill basically gives DHS 90 days (60, really) to set up its portal before the President can declare the need to set up a competing one. This also involves slightly different timing on notice to Congress of whether DHS manages to pull it together in 90 days.

> IN GENERAL.—At any time after certification is submitted under subparagraph (A), the President may designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement a capability and process as described in paragraph (1) in addition to the capability and process developed under such paragraph by the Secretary of

> Homeland Security, if, not fewer than 30 days before making such designation, the President submits to Congress a certification and explanation that—
>
> (I) such designation is necessary to ensure that full, effective, and secure operation of a capability and process for the Federal Government to receive from any non-Federal entity cyber threat indicators or defensive measures under this title;

(1766) The OmniCISA is slightly better on threat of death sharing as it must be specific.

> (iii) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(1768-9) Wow. The regulatory exception is even bigger than it was under CISA. Here's what CISA said (underline added in both):

> (i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this title 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.

And here's what OmniCISA says:

> (i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the

> Federal Government under this title shall not be  used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(1771) The Rule of Construction is more permissive in OmniCISA, too. Compare CISA:

> (c) Construction.—Nothing in this section shall be construed—
>
> (1) to require dismissal of a cause of action against an entity that has engaged in gross negligence or willful misconduct in the course of conducting activities authorized by this title; or

With OmniCISA.

> CONSTRUCTION.—Nothing in this title shall be construed—
>
> (1) to create—
>
> (A) a duty to share a cyber threat indicator or defensive measure; or
>
> (B) a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure; or

Whereas CISA still permitted the government to pursue a company for gross negligence, OmniCISA instead makes clear that companies can ignore cyber information they get shared from the government.

(1771) I'm going to circle back and compare the various oversight reporting from all four bills in more detail. But the big takeaway is that they've stripped a PCLOB review from all 3 of

the underlying bills.

(1782) I'm not sure what this new language does. A lawyer who works in this area thinks it protects Brady obligations. I hope he's right and it's not, instead, a way to eat limits on the use for prosecution.

> (n) CRIMINAL PROSECUTION.—Nothing in this title shall be construed to prevent the disclosure of a cyber threat indicator or defensive measure shared under this title in a case of criminal prosecution, when an applicable provision of Federal, State, tribal, or local law requires disclosure in such case.

(1783) In a (long-overdue) report on how to deal with hacking, OmniCISA takes out a report on this topic specifically done for the Foreign Relations Committee, suggesting this information will remain classified and potentially unavailable to the committees. I guess they have to hide Israel's spying.

> (2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(1785) This is the sunset language. It doesn't seem to sunset anything.

> (a) IN GENERAL.—Except as provided in subsection 3 (b), this title and the amendments made by this title shall be effective during the period beginning on the date of the enactment of this Act and ending on September 30, 2025.