

SO-CALLED OVERSIGHT IN OMNICISA

I did a working thread of the surveillance portion of the version of CISA in the omnibus funding bill here. The short version: it is worse even than CISA was on most counts, although there are a few changes – such as swapping “person” in all the privacy guidelines to “individual” that will have interesting repercussions for non-biological persons.

As I said in that post, I’m going to do a closer look at the privacy provisions that didn’t get stripped from the bill; the biggest change, though, is to eliminate a broad biennial review by the Privacy and Civil Liberties Oversight Board entirely, replacing it with a very narrow assessment, by the Comptroller (!) of whether the privacy scrub is working. Along with the prohibition on PCLOB accessing information from covert ops that got pulled in as part of the Intelligence Authorization incorporated into the bill, it’s clear the Omnibus as a whole aims to undercut PCLOB.

So here’s what counts as “oversight” in OmniCISA. Note, the “appropriate Federal agencies” are the agencies that automatically get information under the sharing system:

- (A) The Department of Commerce
- (B) The Department of Defense
- (C) The Department of Energy
- (D) The Department of Homeland Security
- (E) The Department of Justice
- (F) The Department of the Treasury
- (G) The Office of the Director of National Intelligence

Report on Implementation

**Timing: less than one year
after passage**

**Completed by: heads of
appropriate Federal
agencies**

This is basically a report on whether the information sharing bureaucracy is working to share information effectively. It totally blows off privacy questions and doesn't require an independent assessment. This report includes:

(A) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 105 (c), including any impediments to such real-time sharing.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) The number of cyber threat indicators or defensive measures received through the capability and process developed under section 105(c).

(D) A list of Federal entities that have received cyber threat indicators or defensive measures under this title.

Biennial Report on Compliance

Timing: At least every two years

Completed by: Inspectors General of appropriate Federal agencies, plus Intelligence Community and Council of Inspectors General on Financial Oversight

This report assesses both the same efficacy questions reviewed within a year and privacy protections. But it swaps out a general requirement that the IGs assess, "The degree to which such information may affect the privacy and civil liberties of specific persons," with (D)(ii), below, which is tied to whether information is "related to a cybersecurity threat." Since everything collected would be "related to" (collected because of some technical connection to) a cyberthreat, it basically undercuts the likelihood of a too-broad interpretation of "related to" undercutting privacy.

It includes:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing

cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this title, including a review of the following:

(i) The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this title, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 105(c).

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government entity with the Federal government in contravention of this title, or was shared within the Federal Government in contravention of the guidelines required by this title, including a description of any significant violation of this title.

(iii) The number of times, according to the Attorney General, that information shared under this title was used by a Federal entity to prosecute an offense listed in section 105(d)(5)(A).

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on privacy and civil

liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 105(b)(3)(E).

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this title on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.

Independent Report on Removal of Personal Information

**Timing: Not later than 3
years after passage**

**Completed by: Comptroller
General**

This review will measure “the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this title,” assessing whether the policies and procedures established by the bill are sufficient to address concerns about privacy and civil liberties.