Critical for Cybersecurity and Privacy:

Coons Amendment No. 2652

Ensures DHS Can Apply Effective Privacy Scrub Before Disseminating Indicators

Why CISA’s Current Back-End Privacy Protections Are Inadequate:
CISA’s provisions requiring real-time dissemination of cyber threat indicators throughout the government, and its restraints on the privacy guidelines are contradictory. CISA requires that DHS, or any other federal entity that receives cyber threat indicators, disseminate them in real-time to all appropriate federal entities. While CISA appropriately requires that each federal entity apply privacy guidelines to the indicators, that requirement is rendered ineffective because the application of those guidelines may not result in any delay of dissemination of the information, or in any modification of the information. This means that the privacy guidelines cannot require, or even permit, a brief delay so that the indicators can be reviewed to identify unnecessary or improperly shared PII. Additionally, they cannot permit the removal of any unnecessary or improperly shared PII since that would constitute a modification of those indicators.

Further, the requirement for real-time dissemination, and the restrictions on the privacy guidelines undermine the operational efficacy of the information sharing program, as DHS cautioned in its recent letter to Senator Franken. This is because DHS or any other entity would be prohibited from identifying and withholding from dissemination information that was shared which does not aid cybersecurity, such as information that does not constitute a cyber threat indicator, duplicate indicators, or false positives. CISA would require the dissemination of, and burden security experts with, useless information.

Coons Amendment No. 2652 Resolves This Problem Most Effectively:
The Coons amendment aims to ensure that the government’s cyber-threat program remains operationally efficient and protective of privacy by permitting necessary delays and modifications in the process of disseminating indicators. It would also require that DHS, in its procedures, review cyber threat indicators to identify and remove any unnecessary PII before further disseminating it throughout the government. This additional protection would not apply to other federal entities that directly receive cyber threat indicators under CISA.

The Carper Amendment No. 2615 Resolves Part of the Problem:
Like the Coons amendment, the Carper Amendment No. 2615 would also resolve this concern by ensuring that DHS would be permitted to delay dissemination of cyber threat indicators or modify them in order to apply the privacy procedures. However, the Carper amendment does not include the requirement that DHS review cyber threat indicators and remove all PII unless it is “necessary to identify or describe the cybersecurity threat.” For that reason, OTI prefers the Coons amendment, though we support both.

Neither Amendment Addresses Direct Sharing With NSA:
While both of these amendments resolve the problem that CISA would prohibit DHS from applying effective privacy procedures to cyber threat indicators before disseminating them throughout the government, CISA would still authorize companies to share information with any federal entity. This means that companies could choose to share with agencies like the NSA, CIA, or FBI, and it is unclear how those privacy guidelines would be implemented throughout government.

A chart outlining the types of PII that could be included in cyber threat indicators, and what that PII could reveal, is available at http://bit.ly/1Ku4mDF.

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL AT NEW AMERICA’S OPEN TECHNOLOGY INSTITUTE: greene@opentechnologyinstitute.org