Dangerous for Cybersecurity and Privacy:

Cotton Amendment No. 2581

Reduces Situational Awareness by Incentivizing Decentralized Information Sharing

Why CISA’s Authorization for Sharing Undermines Cybersecurity:

CISA authorizes companies to share cyber threat indicators with any federal entity. It incentivizes companies to share indicators with DHS by offering liability protection. Any companies that opts to forgo that liability protection may share indicators with any federal entity they choose, including intelligence agencies within the Department of Defense like the NSA, pseudo-military agencies like the CIA, or agencies like the EPA, IRS, or OPM, whose functions are entirely unrelated to cybersecurity or which are ill-equipped to protect themselves against cybersecurity threats, let alone protect the indicators that they might receive. This broad authorization is meant to protect existing information sharing relationships, but it is entirely unnecessary. CISA, like other information sharing bills, makes clear that its provisions would not affect or prohibit the continuation of current information sharing relationships or the establishment of new ones.

DHS cautions that by allowing companies to share indicators with whichever agency they chose, it will decentralize information sharing in a way that will seriously undermine federal efforts to enhance cybersecurity. Their concern is that if sharing is authorized with any federal entity, as opposed to only with DHS, “the complexity...and inefficiency of any information sharing program will markedly increase.” DHS further argues that such a broad authorization would result in reduced - not increased - situational awareness, thus “limit[ing] the ability of DHS to connect the dots and proactively recognize emerging risks.” Thus, CISA’s overbroad authorization, allowing companies to share with any federal entity, will undermine the entire purpose of the bill: to increase situational awareness.

How the Cotton Amendment No. 2581 Exacerbates CISA’s Operational Weakness:

The Cotton amendment would significantly exacerbate this operational weakness because it would further decentralize information sharing.

- **Incentivize Information Sharing Directly With FBI:** The Cotton amendment would incentivize companies to share cyber threat indicators directly with the FBI by granting added liability protection. Thus, the result would be reduced situational awareness of cybersecurity threats throughout government.

- **Undermine DHS’s Cybersecurity Mission:** By encouraging companies to share cyber threat indicators directly with the FBI, in lieu of with DHS, the amendment would also further undermine DHS’s role and authorities as the federal government leader for enhancing domestic cybersecurity, which Congress just formally established last year through passage of the Senate’s National Cybersecurity Protection Act (S. 2519). It would also waste taxpayer resources by bypassing the work that has been done to stand up DHS’s National Cybersecurity and Communications Integration Center (NCCIC), which has successfully developed information sharing relationships with many of the nation’s largest industries.

- **Raise Serious Privacy Concerns:** As our nation’s primary domestic intelligence and law enforcement agency, the FBI’s mission is, in part, to investigate U.S. citizens for criminal activity. It would raise serious privacy and civil liberties concerns to place the FBI at the center of the government’s information sharing program, as the Cotton amendment would do. This concern is heightened by the fact that CISA’s current front-end protections could lead to government receipt of significant amounts of innocent Americans’ personal information.


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