

THE ADMINISTRATION STATEMENT ON CISA

I wanted to analyze the Administration's statement on the Cyber Intelligence Sharing Act, which I've reproduced in its entirety below. Opponents of the bill feel the statement betrays Obama's stated (though usually not performed) commitment to civil liberties. And they point to the statement's criticism of defensive measures (see the fifth paragraph below) as one reason the President should oppose this bill but isn't.

Of course, that misconstrues the purpose of such statements, which is to influence the shape of bills as the sausage gets made. As such, this statement commends Richard Burr for concessions he has made, while pointing to the areas where the Administration will push for improvement.

In addition to the defensive measures provision, the chief area the White House is pushing for improvements is on the area where CISA is most vulnerable: on the centrality of DHS to the process.

As such, the Administration supports Senate passage of S. 754, while continuing to work with the Congress as S.754 moves through the legislative process to ensure further important changes are made to the bill, including, but not limited to, preserving the leadership of civilian agencies in domestic cybersecurity.

[snip]

Focusing real-time sharing through one center at DHS enhances situational awareness, facilitates robust privacy controls, and helps to ensure oversight of such sharing. In addition, centralizing this sharing mechanism through DHS will facilitate more effective real-time sharing with other agencies in the most efficient manner.

Therefore, in order to ensure a focused approach and to facilitate streamlined information sharing while ensuring robust privacy protections, the Administration will strongly oppose any amendments that would provide additional liability-protected sharing channels, including expanding any exceptions to the DHS portal. In addition, the Administration remains concerned that the bill's authorization to share with any Federal entity, notwithstanding any other provision of law, weakens the bill's requirement that information be shared with a civilian entity.

Basically, the Administration is still trying to stave off a Tom Cotton effort to let entities share directly with the FBI. Cotton's amendment is bad – but it mostly just exposes the reality of the bill for what it really is.

Moreover, the White House is nuts if they think the current structure will reflect meaningful involvement from DHS. As I noted the other day – and DailyDot reconfirmed today – other agencies (like the FBI) can veto any meaningful involvement from DHS.

So I'm not really surprised by the content of this statement, and the Administration's signals they want to push defensive measures and DHS involvement in a particular direction. I am concerned about their apparent analysis of the state of the bill.

An important building block for improving the Nation's cybersecurity is ensuring that private entities can collaborate to share timely cyber threat information with each other and the Federal Government. In January, the President submitted a legislative proposal to the Congress with the goal of, among other things, facilitating greater information sharing amongst the private sector and with the Federal

Government. The Administration's proposal provides a focused approach to incentivize more cybersecurity information sharing while ensuring the protection of privacy, confidentiality, and civil liberties. As the Administration has previously stated, information sharing legislation must carefully safeguard privacy, confidentiality, and civil liberties, preserve the long-standing respective roles and missions of civilian and intelligence agencies, and provide for appropriate sharing with targeted liability protections. The Administration is encouraged by the strong bipartisan support for cybersecurity information sharing legislation in the Congress.

The Administration appreciates that the Senate Select Committee on Intelligence adopted several amendments to S. 754 to address some of the Administration's most significant concerns and is further encouraged that the bill's sponsor has proposed additional changes on the Senate floor. This work has strengthened the legislation and incorporated important modifications to better protect privacy. As such, the Administration supports Senate passage of S. 754, while continuing to work with the Congress as S.754 moves through the legislative process to ensure further important changes are made to the bill, including, but not limited to, preserving the leadership of civilian agencies in domestic cybersecurity.

The Administration supports S. 754's requirement that an entity sharing information with the Federal Government must share that information through the Department of Homeland Security (DHS) in order to receive liability protections. Moreover, S. 754 requires that such sharing be governed by privacy protection guidelines and that DHS must further disseminate such information in real-time with other Federal agencies. The Administration supports real-time sharing amongst Federal agencies with appropriate privacy protections, and is currently developing such a capability at DHS. Focusing real-time sharing through one center at

DHS enhances situational awareness, facilitates robust privacy controls, and helps to ensure oversight of such sharing. In addition, centralizing this sharing mechanism through DHS will facilitate more effective real-time sharing with other agencies in the most efficient manner.

Therefore, in order to ensure a focused approach and to facilitate streamlined information sharing while ensuring robust privacy protections, the Administration will strongly oppose any amendments that would provide additional liability-protected sharing channels, including expanding any exceptions to the DHS portal. In addition, the Administration remains concerned that the bill's authorization to share with any Federal entity, notwithstanding any other provision of law, weakens the bill's requirement that information be shared with a civilian entity. This remains a significant concern, and the Administration is eager to work with the Congress to seek a workable solution.

S. 754 authorizes the use of certain potentially disruptive defensive measures in response to network incidents, provisions that were not included in the Administration's proposal. The use of defensive measures raises significant legal, policy, and diplomatic concerns and, without appropriate safeguards, can have a direct deleterious impact on foreign policy, the integrity of information systems, and cybersecurity. The Administration is encouraged, however, that the bill's sponsor has proposed changes that would limit an entity from employing a defensive measure that would provide it unauthorized access to another entity's network. Though the Administration remains concerned that the bill's authorization to operate defensive measures may prevent the application of other laws such as State common-law tort remedies, it is encouraged that the additional changes will help to appropriately constrain the use of defensive measures. The Administration is committed to continue working with stakeholders to address remaining concerns.

The Administration commends the Committee for recognizing that cybersecurity requires a whole-of-government approach and that information must be appropriately shared within the Federal Government. This sharing must be consistent with certain narrow cybersecurity use restrictions, as well as privacy, confidentiality, and civil liberties protections and transparent oversight. The Administration commends the Committee for requiring that intra-governmental sharing be governed by a set of policies and procedures developed by the Federal Government to protect privacy and civil liberties. The Administration is encouraged that the bill's sponsor has proposed changes that would preserve the Federal Government's ability to implement privacy protective policies and procedures. The Administration is encouraged by changes the bill's sponsor has proposed to ensure that information sharing provided for in the bill is narrowly focused on the important purpose of this bill, the protection of information systems and information from cybersecurity threats and security vulnerabilities. Finally, the Administration is pleased that S.754 includes provisions that will improve the cybersecurity of Federal networks and systems. Consistent with the bill's requirements, the Administration will implement this authority in a manner that both enhances cybersecurity and continues to protect the confidentiality, availability, and integrity of Federal agencies' data.

Information sharing is one piece of a larger suite of legislation needed to provide the private sector, the Federal Government, and law enforcement with the necessary tools to combat cyber threats, and create for consumers and businesses a strong and consistent notification standard for breaches of personal data. In addition to updating information sharing statutes, the Congress should incorporate privacy, confidentiality protection, and civil liberties safeguards into all aspects of cybersecurity legislation.