CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

April 14, 2015

S. 754
Cybersecurity Information Sharing Act of 2015

As reported by the Senate Select Committee on Intelligence on March 17, 2015

S. 754 would require the government to establish procedures to be followed when information on cyber threats is shared between the government and nonfederal entities. The bill also would require the government to audit the process for sharing information and would require additional reports to the Congress on cyber information sharing. CBO anticipates that approximately 20 additional personnel would be needed to administer the program, prepare the required reports and manage the exchange of information. Based on information from the Department of Homeland Security, the Office of Management and Budget, and other cybersecurity experts, CBO estimates that the requirements imposed by S. 754 would cost approximately $20 million over the 2016-2020 period, assuming appropriation of the estimated amounts.

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. Enacting S. 754 would affect direct spending and revenues because the bill would allow information shared with the government to be used in investigating and prosecuting certain violent crimes. Any additional convictions for such offenses could increase the collection of fines. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent. CBO expects that additional revenues and direct spending would not be significant because of the small number of cases likely to be effected.

S. 754 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use cyber threat information. Doing so would prevent public and private entities from seeking compensation for damages from those protected entities. The bill also would impose additional intergovernmental mandates on state and local governments by preempting disclosure and liability laws and laws that restrict cybersecurity monitoring, sharing, and countermeasure activities authorized by the bill.

Because of uncertainty about the number of cases that would be limited and any foregone compensation that would result from compensatory damages that might otherwise go to private-sector entities, CBO cannot determine whether the costs of the mandate would

exceed annual thresholds established in UMRA for private-sector mandates ($154 million in 2015, adjusted annually for inflation). The amount of cybersecurity information shared by state, local, and tribal governments is much smaller than that shared by the private sector, and public entities are much less likely to bring lawsuits as plaintiffs in such cases. Consequently, CBO estimates that the aggregate costs of the mandates on public entities would fall below the threshold for intergovernmental mandates ($77 million in 2015, adjusted annually for inflation).

On April 13, 2015, CBO transmitted a cost estimate for H.R. 1560 as ordered reported by the House Permanent Select Committee on Intelligence on March 26, 2015. Differences in the estimated costs reflect differences in the bills. Specifically, H.R. 1560 contains provisions that would establish a National Cyber Threat Intelligence Integration Center and would make the federal government liable if federal agencies or departments violated privacy and civil liberty guidelines also required by that bill. Those provisions are not included in S. 754.

The CBO staff contact for this estimate is Jason Wheelock. The estimate was approved by Theresa Gullo, Assistant Director for Budget Analysis.