CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

April 13, 2015

H.R. 1560
Protecting Cyber Networks Act

As ordered reported by the House Permanent Select Committee on Intelligence on March 26, 2015

SUMMARY

H.R. 1560 would establish within the Office of the Director of National Intelligence (ODNI) a center that would be responsible for analyzing and integrating information from the intelligence community related to cyber threats. In addition, the bill would require the government to establish procedures for sharing information and data on cyber threats between the federal government and nonfederal entities. CBO estimates that implementing the bill would cost $186 million over the 2016-2020 period, assuming appropriation of the estimated amounts.

In addition, the bill would allow information shared with the government to be used in certain criminal prosecutions, which could increase federal revenues from fines as well as direct spending from the Crime Victims Fund. However, CBO anticipates that the number of cases that could be affected would be small and that any additional revenues and spending would be insignificant. Finally, section 5 of H.R. 1560 would make the government liable if an agency or department were to violate the privacy and civil liberty guidelines required by the bill. While such liability could result in additional direct spending, CBO does not have sufficient basis to estimate the type or frequency of violations or budgetary impact that might occur if the legislation was enacted. Because the bill would affect direct spending and revenues, pay-as-you-go procedure apply.

H.R. 1560 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 if they share or use cybersecurity information. The bill also would impose additional intergovernmental mandates on state and local governments by preempting disclosure and liability laws and by preempting any laws that restrict 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 the 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).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary effect of H.R. 1560 is shown in the following table. The costs of this legislation fall within budget function 050 (national defense).

	By Fiscal Year, in Millions of Dollars					
	2016	2017	2018	2019	2020	2016-2020
National Cyber Threat Intelligence and Integration Center						
Estimated Authorization Level	35	36	37	38	39	185
Estimated Outlays	23	33	35	37	38	166
Oversight, Administration, and Reporting						
Estimated Authorization Level	4	4	4	4	4	20
Estimated Outlays	4	4	4	4	4	20
Total Changes						
Estimated Authorization Level	39	40	41	42	43	205
Estimated Outlays	27	37	39	41	42	186

BASIS OF ESTIMATE

For this estimate, CBO assumes that the legislation will be enacted near the end of fiscal year 2015, and that outlays will be similar to historical spending patterns for similar activities.

National Cyber Threat Intelligence and Integration Center

The bill would establish a National Cyber Threat Intelligence Integration Center (CTIIC) that would be responsible for analyzing, integrating, and disseminating intelligence on cyber threats within the federal government. In February, based on authority in current law to establish intelligence centers, the President announced his intention to establish a CTIIC within the ODNI; however, the process for establishing and creating an operational center has not been completed. H.R. 1560 would require such a center to have a maximum of 50 permanent positions. CBO estimates, based on publicly available information regarding the planned center, the personnel ceiling in H.R. 1560, and budget data from the Office of Management and Budget (OMB), that implementing this provision would cost approximately $166 million over the 2016-2020 period, assuming appropriation of the estimated amounts.

Oversight, Administration, and Reporting

H.R. 1560 also would require the government to establish procedures to be followed when information on cyber threats is shared between the government and nonfederal entities, such as requiring personal data to be expunged from shared information. The bill also would require the government to audit the process for sharing information with nonfederal entities and would require additional reports to the Congress on cyber intelligence 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 between the government and nonfederal entities (such as state, local, and tribal governments and private companies). Based on information from the Department of Homeland Security, OMB, and other cybersecurity experts, CBO estimates that the requirements imposed by H.R. 1560 would cost approximately $20 million over the 2016-2020 period, assuming appropriation of the estimated amounts.

PAY-AS-YOU-GO CONSIDERATIONS:

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. Enacting H.R. 1560 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 that result 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.

In addition, section 5 of H.R. 1560 would allow a person to collect damages and attorney's fees if a federal agency or department violates the privacy and civil liberty guidelines required to be issued under the bill. Any costs to the federal government for such cases would constitute direct spending. However, because the types of violations and the frequency with which they might occur would depend on guidelines that have not yet been established, CBO does not have a sufficient basis to estimate the effect of this provision.

INTERGOVERNMENTAL AND PRIVATE-SECTOR IMPACT

H.R. 1560 would impose intergovernmental and private-sector mandates as defined in 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 for sharing or using cybersecurity information. The bill also would impose additional intergovernmental mandates on state and local governments by preempting disclosure and liability laws and by preempting any laws that restrict the 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 the 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).

ESTIMATE PREPARED BY:

Federal Costs: Jason Wheelock
Impact on State, Local, and Tribal Governments: Jon Sperl
Impact on the Private Sector: Paige Piper/Bach

ESTIMATE APPROVED BY:

Theresa Gullo
Assistant Director for Budget Analysis