CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

July 12, 2010

S. 773
Cybersecurity Act of 2010

As ordered reported by the Senate Committee on Commerce, Science, and Transportation on March 24, 2010

SUMMARY

S. 773 would authorize several National Science Foundation (NSF) grant and scholarship programs aimed at enhancing cybersecurity (the protection of computers and computer networks from unauthorized access) through expanded research and workforce development. The bill also would authorize the National Institute of Standards and Technology (NIST) to carry out certain activities to promote the development of new cybersecurity technologies and to enhance public awareness of cybersecurity issues. In addition, the bill would direct the President to develop and implement a comprehensive cybersecurity strategy for the federal government. Finally, the legislation would codify certain ongoing activities related to cybersecurity.

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 773 would cost $1.4 billion over the 2011-2015 period. Pay-as-you-go procedures do not apply to this legislation because it would not affect direct spending or revenues.

S. 773 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on owners and operators of information systems designated as critical infrastructure by the President. Owners and operators of such systems would have to comply with new security standards and procedures. Because the number of entities subject to the mandates would be large, and the costs of complying with some of the mandates in the bill would be substantial, CBO estimates that the costs to comply would well exceed the annual thresholds established in UMRA for intergovernmental and private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

CBO has not reviewed section 201(b) of the bill for mandates. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that the provisions of section 201(b) fall within that exclusion because they would allow the President to declare a cybersecurity emergency and implement emergency-response and restoration plans.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 773 is shown in the following table. The costs of this legislation fall within budget functions 250 (general science, space, and technology), 370 (commerce and housing credit), and 800 (general government).

	By Fiscal Year, in Millions of Dollars					
	2011	2012	2013	2014	2015	2011-2015
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
National Science Foundation Activities						
Authorization Level	339	356	371	388	0	1,454
Estimated Outlays	61	210	295	338	297	1,201
Department of Commerce Activities						
Estimated Authorization Level	38	48	58	68	8	220
Estimated Outlays	20	34	44	55	45	198
Other Activities						
Estimated Authorization Level	7	6	6	6	6	31
Estimated Outlays	6	6	6	6	6	30
Total Spending Under S. 773						
Estimated Authorization Level	384	410	435	462	14	1,705
Estimated Outlays	87	250	345	399	348	1,429

BASIS OF ESTIMATE

For this estimate, CBO assumes that the legislation will be enacted in 2010 and that the necessary amounts will be appropriated for each fiscal year. Estimated outlays are based on historical spending patterns for similar programs.

National Science Foundation Activities

S. 773 would authorize appropriations totaling about $1.2 billion over the 2011-2014 period for several existing NSF programs related to cybersecurity research. The bill also would authorize the appropriation of $250 million over that period for the agency to provide scholarships to students who pursue higher education in fields related to cybersecurity. Finally, the bill would authorize the appropriation of $2 million a year over the 2011-2012 period to provide grants for higher education institutions to develop cybersecurity curricula. Based on information from NSF and assuming appropriation of

the authorized amounts, CBO estimates that implementing the NSF programs authorized under the bill would cost $1.2 billion over the 2011-2015 period.

Department of Commerce Activities

S. 773 would authorize the appropriation of $15 million a year over the 2011-2014 period for NIST to award cash prizes to individuals who develop innovative cybersecurity technologies. The bill also would require the agency to establish regional cybersecurity centers that would assist businesses in implementing cybersecurity best practices. In addition, the legislation would require NIST to establish a program to promote cybersecurity awareness and education. Finally, the bill would require the Secretary of Commerce to develop a tracking system to provide the real-time cybersecurity status of all federal agencies within the Department of Commerce. Based on information regarding the cost of implementing similar programs, CBO estimates that carrying out the provisions affecting the Department of Commerce would cost $198 million over the 2011-2015 period, assuming appropriation of the authorized and necessary amounts.

Other Activities

S. 773 would direct the President to establish a national cybersecurity strategy and to conduct biennial reviews to assess the nation's cybersecurity posture. The legislation also would require the President to appoint a panel of academic and industry experts to advise the Office of Science and Technology Policy on issues related to cybersecurity. Finally, the bill would require a study by the National Academies to assess workforce development efforts related to cybersecurity. Based on information regarding the cost of similar activities, CBO estimates that implementing those provisions would cost $30 million over the 2011-2015 period.

PAY-AS-YOU-GO CONSIDERATIONS: None.

INTERGOVERNMENTAL AND PRIVATE-SECTOR IMPACT

Mandates that Apply to Both Intergovernmental and Private-Sector Entities

S. 773 would impose intergovernmental and private-sector mandates, as defined in UMRA, on owners and operators of information systems designated as critical infrastructure by the President. Critical infrastructure could include information systems for public and private transportation systems, police and fire departments, airports, hospitals, electric utilities, health departments, water systems, and financial companies.

The bill would require those entities to:

- Train employees working in cybersecurity to meet new certification requirements;

- Comply with risk-management techniques and best practices to be established for cybersecurity; and

- Audit their compliance with those requirements on a semi-annual basis and report the results of those audits to the federal government.

The costs of complying with the mandates would depend on future regulations, the extent to which the regulations would impose requirements that differ from current practice, and which entities would be subject to those requirements. Based on information from industry sources, the cost of conducting a cybersecurity audit could range from $30,000 to millions of dollars per entity, depending on the size of the entity and the nature and scope of the audit. For example, such an audit could involve ensuring compliance with firewall, encryption, and data storage and transfer requirements, among other risk-management techniques. Based on information from government and industry sources, more than 50,000 public entities could be subject to the mandates. Further, according to a study by the Government Accountability Office, the private sector owns more than 85 percent of the nation's critical infrastructure. Because the number of entities subject to the mandates could be large and the costs of complying with some of the mandates in the bill would be substantial, CBO estimates that the aggregate costs to comply would well exceed the annual thresholds established in UMRA for intergovernmental and private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

Provisions Excluded under UMRA

CBO has not reviewed section 201(b) of the bill for mandates. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined the provisions of section 201(b) fall within that exclusion because they would allow the President to declare a cybersecurity emergency and implement emergency-response and restoration plans.

Other Impacts on State and Local Governments

The bill would benefit public institutions of higher education by authorizing grants for cybersecurity programs. Any costs that those entities incur would result from complying with conditions of federal assistance.

PREVIOUS CBO ESTIMATE

On December 10, 2009, CBO transmitted a cost estimate for H.R. 4061, the Cybersecurity Enhancement Act of 2009, as ordered reported by the House Committee on Science and Technology on November 18, 2009. S. 773 contains several provisions that were included in H.R. 4061; however, the authorization levels for those provisions are different. In addition, S. 773 contains additional provisions that were not included in H.R. 4061. The CBO cost estimates reflect those differences.

ESTIMATE PREPARED BY:

Federal Costs: Jeff LaFave
Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle
Impact on the Private Sector: Samuel Wice

ESTIMATE APPROVED BY:

Peter H. Fontaine
Assistant Director for Budget Analysis