



CONGRESSIONAL BUDGET OFFICE  
COST ESTIMATE

November 5, 2013

**S. 1353**  
**Cybersecurity Act of 2013**

*As ordered reported by the Senate Committee on Commerce, Science,  
and Transportation on July 30, 2013*

**SUMMARY**

S. 1353 would direct several agencies within the federal government to take certain actions to facilitate public-private cooperation on cybersecurity standards, improve research and development in cybersecurity technologies, and further education and public awareness on cybersecurity matters. Several of the bill's requirements pertain to existing or planned programs and initiatives, while others create new requirements or expand the scope of existing efforts.

CBO estimates that implementing S. 1353 would cost \$56 million over the 2014-2018 period, assuming appropriation of the necessary amounts. Pay-as-you-go procedures do not apply to this legislation because it would not affect direct spending or revenues.

S. 1353 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

**ESTIMATED COST TO THE FEDERAL GOVERNMENT**

The estimated budgetary impact of S. 1353 is shown in the following table. The costs of this legislation fall within budget functions 250 (general science, space, and technology) and 370 (commerce and housing credit).

|  | By Fiscal Year, in Millions of Dollars |      |      |      |      | 2014-<br>2018 |
|--|--|------|------|------|------|---------------|
|  | 2014                                   | 2015 | 2016 | 2017 | 2018 |               |
| <b>CHANGES IN SPENDING SUBJECT TO APPROPRIATION</b>      |  |      |      |      |      |               |
| Cybersecurity Standards and Public-Private Collaboration |  |      |      |      |      |               |
| Estimated Authorization Level                            | *                                      | 1    | *    | *    | 1    | 2             |
| Estimated Outlays  | *                                      | 1    | *    | *    | 1    | 2             |
| Cybersecurity Research and Development                   |  |      |      |      |      |               |
| Estimated Authorization Level                            | *                                      | 14   | 13   | 14   | 13   | 55            |
| Estimated Outlays  | *                                      | 2    | 8    | 12   | 12   | 35            |
| Cybersecurity Education, Training, and Public Awareness  |  |      |      |      |      |               |
| Estimated Authorization Level                            | 4                                      | 4    | 4    | 4    | 4    | 20            |
| Estimated Outlays  | 3                                      | 4    | 4    | 4    | 4    | 19            |
| Total Changes  |  |      |      |      |      |               |
| Estimated Authorization Level                            | 5                                      | 19   | 17   | 18   | 18   | 77            |
| Estimated Outlays  | 4                                      | 7    | 12   | 16   | 17   | 56            |

Note: Components may not sum to totals because of rounding. \* = less than \$500,000.

## **BASIS OF ESTIMATE**

For this estimate, CBO assumes that the bill will be enacted early in 2014, the necessary amounts will be appropriated each year, and spending will follow historical patterns for similar activities.

### **Cybersecurity Standards and Public-Private Collaboration**

Title I would codify certain elements of Executive Order 13636 by directing the National Institute of Standards and Technology (NIST) to develop a framework of voluntary standards designed to reduce risks arising from cyberattacks on critical infrastructure that is privately owned and operated. The agency expects to spend about \$6 million to develop the standards (the preliminary framework was completed in October 2013) and anticipates spending a similar amount annually to review and update the framework as required by the executive order. Based on information from the agency, CBO estimates that codifying the requirements of the executive order would not significantly increase the agency's costs.

Title I also would require the Government Accountability Office (GAO) to assess progress made by NIST in developing the framework and the private sector in adopting the standards; GAO also would be required to prepare a summary of its findings and report to the Congress every two years. CBO estimates that implementing this provision would cost \$2 million over the 2014-2018 period, assuming the availability of appropriated funds.

### **Cybersecurity Research and Development**

Title II would require the Director of the National Science Foundation (NSF) to review existing infrastructure used to test cybersecurity technologies within one year of the bill's enactment. Based on the results of the review, the NSF would be authorized to award grants to establish additional infrastructure to test cybersecurity technologies. Based on information provided by the agency, CBO estimates that implementing this provision would cost \$33 million over the 2014-2018 period, assuming the appropriation of the necessary amounts.

Title II also would require the Director of the Office of Science and Technology Policy (OSTP) to develop a federal cybersecurity research and development plan in consultation with nonfederal entities. Under the legislation, the director would be required to update the plan and report to the Congress every three years. Based on information provided by OSTP, CBO estimates that implementing this provision would cost about \$2 million over the next five years.

### **Cybersecurity Education, Training, and Public Awareness**

Title III would require the Director of the NSF to contract with the National Academy of Sciences (NAS) to conduct a study of education, training, and certification programs for the development of professionals in the areas of information infrastructure and cybersecurity. Based on information from the NAS, CBO estimates that implementing this provision of title III would cost \$1 million over the 2014-2018 period, assuming appropriation of the necessary amounts.

Other provisions of title III would require the Director of the NSF to continue a scholarship-for-service program to train professionals to meet the cybersecurity needs of federal, state, local, and tribal governments. This title also would require several agencies, including the Department of Commerce, NSF, and the Department of Homeland Security, to support competitions to identify and recruit individuals to enhance innovation in basic and applied cybersecurity that can be used to advance the mission of the agency. Based on information from those agencies, CBO estimates that implementing those provisions would not significantly increase discretionary spending over the 2014-2018 period because those activities are already occurring under current law.

Title IV would require NIST to continue to coordinate a national campaign to increase public awareness of cybersecurity threats. The agency also would be required to develop and implement a strategic plan to guide federal agencies' support of the campaign. Based on information from NIST, CBO expects that implementing those requirements would cost \$18 million over the 2014-2018 period, assuming appropriation of the necessary amounts, for personnel and administrative costs.

**PAY-AS-YOU-GO CONSIDERATIONS:** None.

### **INTERGOVERNMENTAL AND PRIVATE-SECTOR IMPACT**

S. 1353 contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments

### **ESTIMATE PREPARED BY:**

Federal Costs: Susan Willie and Martin von Gnechten  
Impact on State, Local, and Tribal Governments: J'nell L. Blanco  
Impact on the Private Sector: Marin Burnett

### **ESTIMATE APPROVED BY:**

Theresa Gullo  
Deputy Assistant Director for Budget Analysis