CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

November 17, 2010

S. 3480
Protecting Cyberspace as a National Asset Act of 2010

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on June 24, 2010

SUMMARY

S. 3480 would amend the Federal Information Security Management Act of 2002 (FISMA) to strengthen and coordinate security controls over computer information systems across federal civilian agencies. In addition, the legislation would aim to increase the security of privately owned computer networks for online communication and prevent intentional disruptions of such networks. S. 3480 would establish new offices, require additional testing of computer systems, and provide federal agencies with new authorities and responsibilities related to information security.

Based on information from the Department of Homeland Security (DHS), the Office of Management and Budget (OMB), and other major agencies involved in cybersecurity, CBO estimates that implementing S. 3480 would cost $1.5 billion over the 2011-2015 period, assuming appropriation of the necessary amounts. Most of those funds would be spent on salaries, expenses, and computer hardware and software.

The bill would, under certain circumstances, indemnify owners of critical infrastructure who implement emergency-response plans required by the federal government. CBO estimates that this authority would increase direct spending by $10 million over the 2011-2020 period to pay claims against the U.S. government; therefore, pay-as-you-go procedures apply. Enacting the legislation would not affect revenues.

S. 3480 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 DHS. Owners and operators of such systems would have to comply with new security standards and procedures. The bill also would impose a mandate by limiting the damages that users of critical infrastructure can seek from owners and operators of such systems for incidents related to cyber risks.

Because the cost to comply with new security standards would depend on future regulations and because of uncertainty about the number of such claims that would be

filed in the absence of this legislation, CBO cannot determine whether the aggregate cost of the mandates in the bill would exceed the annual thresholds established in UMRA for intergovernmental or private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

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

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 3480 is shown in the following table. The costs of this legislation fall within budget functions 050 (national defense) and 800 (general government).

	By Fiscal Year, in Millions of Dollars					
	2011	2012	2013	2014	2015	2011-2015
CHANGES IN SPENDING SUBJECT TO APPROPRIATION[a]						
Changes to Information Security Management						
Estimated Authorization Level	100	175	225	300	325	1,125
Estimated Outlays	80	160	215	285	320	1,060
National Center for Cybersecurity and Communications						
Estimated Authorization Level	50	50	51	52	53	256
Estimated Outlays	27	44	49	50	51	221
Office of Cyberspace Policy						
Estimated Authorization Level	10	20	30	31	32	123
Estimated Outlays	8	18	28	30	31	115
Other Provisions						
Estimated Authorization Level	20	20	20	20	20	100
Estimated Outlays	19	20	20	20	20	99
Total Changes						
Estimated Authorization Level	180	265	326	403	430	1,604
Estimated Outlays	134	242	312	385	422	1,495

Note: Components may not sum to totals because of rounding.

a. S. 3480 also would increase direct spending by $10 million over the 2016-2020 period, CBO estimates, because of a provision that would, under certain circumstances, indemnify owners of critical infrastructure who comply with government-ordered procedures during a cyber emergency.

BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted in calendar year 2010, that the necessary amounts will be appropriated each year, and that spending will follow historical patterns for salaries and expenses related to securing federal information systems. CBO estimates that implementing S. 3480 would cost about $1.5 billion over the 2011-2015 period.

Changes to Information Security Management

Under S. 3480, agencies would be required to perform new activities, including:

- Automated monitoring of systems to secure information;
- Testing of information security controls;
- Evaluating information security programs and practices; and
- Establishing a Federal Information Security Task Force.

Most of the provisions of the bill would expand practices already being carried out by the federal government under FISMA. In 2009, federal agencies spent nearly $7 billion on such activities. That amount includes about $300 million for certification and accreditation activities (the processes used by all federal agencies to assess, test, and accept the security controls that protect information systems). FISMA also sets forth a comprehensive framework for ensuring that security controls for information resources that support federal operations and assets are effective. Specifically, FISMA requires the head of each agency to provide protections that would be commensurate with the risk and magnitude of harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information and systems used or operated by each agency.

Based on information from OMB and other selected agencies, CBO estimates that when fully implemented, the new activities specified in S. 3480 would increase federal spending for FISMA activities by about 4 percent—about $300 million annually. CBO expects that it would take about four years to reach that level of effort for the thousands of federal computer systems currently operating. Over the 2011-2015 period, we estimate that implementing those new requirements and authorities would cost about $1 billion, assuming appropriation of the necessary amounts.

National Center for Cybersecurity and Communications

Section 201 would establish the National Center for Cybersecurity and Communications (NCCC) within the Department of Homeland Security. The new center would be responsible for leading DHS's efforts to secure federal civilian networks and work with state and local governments and the private sector to secure the nation's information infrastructure. The bill would transfer the authorities, personnel, and other assets of DHS's National Cybersecurity Division, the Office of Emergency Communications, and the National Communications System to the NCCC.

Although the bill would transfer existing assets and funds to the NCCC, CBO anticipates that the mission of the new NCCC would require additional funding to implement. In particular, the bill would require more extensive testing of federal and private information systems. In its 2011 budget justification, DHS outlined a plan to spend approximately $10 million to conduct 27 assessments of the federal government's information systems. Based on that information, CBO estimates that conducting the cyber assessments envisioned by the bill would cost an additional $220 million over the 2011-2015 period, assuming appropriation of the necessary amounts.

Office of Cyberspace Policy

The Executive Office of the President currently employs a coordinator to manage cybersecurity policies. Title I would expand that role and establish an Office of Cyberspace Policy within the Executive Office of the President. The office would advise the President and help coordinate all cybersecurity regulations, standards, and strategies.

Based on information provided by OMB and the cost of similar offices and programs, CBO estimates that creating the new office would cost about $30 million a year once fully implemented. We expect that the office would steadily expand its budget and staff over three years before it reached that level of effort and estimate that implementing the title would cost $115 million over the 2011-2015 period.

Other Provisions

The legislation also would require federal agencies to:

- Assess the skills of information security employees;
- Prepare plans to train information security workers; and
- Establish a National Cybersecurity Advisory Council.

Based on information from DHS and OMB, CBO estimates that implementing those provisions would cost about $20 million annually over the 2011-2015 period.

Direct Spending

Under the bill, the Director of the NCCC would be authorized to require owners of critical infrastructure (assets essential to society and the economy, including facilities for energy production, telecommunications, public health, and food and water supply) to implement response plans if a national cyber emergency was declared by the President. Although the probability is very low, such a plan could involve an interruption of service in the telecommunications or electric power sectors. Section 201 would indemnify the owners of such infrastructure in civil actions if implementation of those response plans resulted in the serious physical injury or death of an individual or substantial damage or destruction of an individual's primary residence. Any claims against the government related to indemnifying such entities would be paid from the Judgment Fund (a permanent, indefinite appropriation for claims and judgments against the United States) and would be considered direct spending.

CBO has determined that cyber attacks on electrical utilities and telecommunications providers would present the biggest potential for liability under this section because an interruption of service in those sectors could affect emergency response services. Because there is no relevant historical data on which to determine the probability of an attack that would trigger the implementation of such plans, CBO consulted with numerous cyber security and cyber insurance experts. CBO based its estimate of the costs of indemnifying entities on information derived from those discussions including the likelihood of a widespread, high-impact cyber event and on an analysis of the potential liability if there was an interruption of electrical power or telecommunications services in a large metropolitan area. Based on that analysis, CBO estimates that enacting this provision would increase direct spending by $10 million over the 2016-2020 period. Since CBO cannot predict the value of claims that might be paid in any particular year, our estimate of the cost represents the sum of a weighted average of payments from the Judgment Fund over the 2016-2020 period. Since CBO anticipates that any potential litigation involving such claims would be lengthy, we estimate that this provision would not affect direct spending over the 2011-2015 period.

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. S. 3480 could affect direct spending by agencies not funded through annual appropriations, such as the Tennessee Valley Authority and the Bonneville Power Administration; therefore, pay-as-you-go procedures apply. CBO estimates, however, that any net increase in annual

spending by those agencies would not be significant and enacting the legislation would not affect revenues.

In addition, the bill would affect direct spending because of a provision that would, under certain circumstances, indemnify owners of critical infrastructure who comply with government-ordered procedures during a cyber emergency. CBO estimates that enacting that provision would increase direct spending by $10 million over the 2016-2020 period.

In total, the net budgetary changes in the bill subject to pay-as-you-go procedures would be insignificant over the 2011-2015 period and $10 million over the 2016-2020 period.

INTERGOVERNMENTAL AND PRIVATE-SECTOR IMPACT

S. 3480 contains several intergovernmental and private-sector mandates, as defined in UMRA. Because of uncertainty about the nature or scope of some of the mandates, CBO cannot determine whether the aggregate cost of the mandates in the bill would exceed the annual thresholds established in UMRA for intergovernmental or private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

Mandates that Apply to Both Intergovernmental and Private-Sector Entities

Cyber Protection. The bill would impose intergovernmental and private-sector mandates, as defined in UMRA, on owners and operators of information systems designated as critical infrastructure by DHS. Owners and operators of such systems would have to comply with new security standards and reporting requirements. 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. Based on information from government and industry sources, CBO estimates that more than 50,000 public entities could be subject to the mandates. Further, a study by the Government Accountability Office indicates that the private sector owns more than 85 percent of the nation’s critical infrastructure.

The bill would require owners and operators of information systems designated as critical infrastructure to comply with standards for managing cybersecurity risks and to certify in writing that they are in compliance with those standards. Because the costs of complying with the mandate would depend on future regulations, CBO has no basis for estimating the cost of the mandates on public or private-sector entities, primarily because it is not clear which entities would be affected or whether future regulations would differ significantly from current practices.

S. 3480 also would require affected entities to report incidents that could indicate a risk to cybersecurity. CBO estimates that the cost of complying with this mandate to public and private entities would be small relative to the annual thresholds.

Liability Limits. The bill also would impose a mandate by limiting the damages that may be recovered from owners and operators of critical infrastructure for incidents related to cyber risks. Compensation for certain damages would only be limited for claims against owners and operators that comply with the cybersecurity standards issued by DHS. Because we are uncertain about both the value of awards in such cases and the number of claims that would be filed in the absence of this legislation, CBO cannot determine whether the cost of the mandate would exceed the annual thresholds for intergovernmental or private-sector mandates.

Provisions Excluded under UMRA

CBO has not reviewed provisions of the bill that would allow the President to declare a national cyber emergency and implement emergency-response and restoration plans. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that those provisions fall within that exclusion.

ESTIMATE PREPARED BY:

Federal Costs: Matthew Pickford and Jason Wheelock
Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle
Impact on the Private Sector: Samuel Wice

ESTIMATE APPROVED BY:

Theresa Gullo
Deputy Assistant Director for Budget Analysis