



CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

March 29, 2000

S. 1993 **Government Information Security Act**

*As ordered reported by the Senate Committee on Governmental Affairs
on March 23, 2000*

S. 1993 would require federal agencies to perform certain tasks to improve the security of their computer systems. Subject to the availability of appropriated funds, CBO estimates that implementing S. 1993 would cost federal agencies between \$10 million and \$15 million annually to audit their security programs and practices. While this work should both increase the cost-effectiveness of federal security systems and reduce the likelihood of costly service disruptions, CBO has no basis for estimating the amount of potential savings from such improvements.

The bill would not affect direct spending or receipts, so pay-as-you-go procedures would not apply. S. 1993 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

S. 1993 would require federal agencies to develop a risk-based program for ensuring the security of their information systems, including designating a senior official to oversee the program, periodically assessing and testing their systems, and providing training to personnel. In addition, the bill would require that either an inspector general or independent evaluator annually audit an agency's security programs and practices. S. 1993 also would specify the responsibilities of particular agencies in securing the government's information systems, including the National Institute of Standards and Technology, the Department of Justice, and the General Services Administration. Finally, the bill would require the Office of Management and Budget (OMB) to establish policies for implementing its provisions.

Most of S. 1993 would codify and centralize current practice, including directions provided in the Government Security Act, OMB Circular No. A-130 (Management of Federal Information Resources), and Presidential Decision Directive 63, concerning the protection of critical infrastructure. While some agencies already evaluate portions of their information systems through the financial audits required by the Chief Financial Officers (CFO) Act and

the security reviews required by OMB Circular No. A-130, the bill would call for agencies to audit their systems more extensively and regularly.

Based on information from the General Accounting Office, which has reviewed the security practices of federal agencies, and OMB, CBO estimates that requiring the annual audits would increase agency costs by between \$10 million and \$15 million annually, subject to the availability of appropriated funds. That estimate assumes that the 25 largest federal departments and agencies (those with appointed CFOs) would regularly test the general and management controls of critical, nonfinancial operations. We estimate that the evaluation of between 55 and 75 computer systems operated by these agencies would cost around \$150,000 each, or a total of around \$10 million annually. Although much uncertainty exists as to the number and complexity of computer operations that smaller agencies would need to evaluate, as well as the extent that such evaluations already take place, CBO expects that applying the audit requirement to them would increase the provision's cost by as much as 50 percent.

In addition, the audits should both improve the cost-effectiveness of federal security systems and decrease the likelihood of costly service disruptions. CBO, however, cannot estimate the amount of potential savings from such improvements.

The CBO staff contact is John R. Righter. This estimate was approved by Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.