September 2009

INFORMATION SECURITY

Concerted Effort Needed to Improve Federal Performance Measures

GAO Accountability•Integrity•Reliability

Highlights

Highlights of GAO-09-617, a report to the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Information security is a critical consideration for federal agencies, which depend on information systems to carry out their missions. Increases in reports of security incidents demonstrate the urgency of adequately protecting the federal government's data and information systems. Agencies are required to report to the Office of Management and Budget (OMB) on their information security programs, and OMB is to report results to Congress. Agencies have reported progress in carrying out their activities and have used a variety of measures as the basis of that reporting. GAO was asked to (1) describe key types and attributes of performance measures, (2) identify practices of leading organizations for developing and using measures to guide and monitor information security activities, (3) identify the measures used by federal agencies and how they are developed, and (4) assess the federal government's practices for informing Congress on the effectiveness of information security programs. To do this, GAO met with leading organizations, consulted with experts, and reviewed major federal agencies' policies and practices.

What GAO Recommends

GAO is recommending that OMB guide agencies to develop balanced portfolios of measures and improve collection and reporting of measures to Congress. OMB generally agreed with the contents and recommendations of this report.

View GAO-09-617 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Experts and leading organizations (nationally known organizations, academic institutions, and state agencies with enterprisewide information security measurement programs) have identified key types and attributes of successful information security measures. These measures fell into three major types: (1) compliance with policies, standards, or legal and regulatory requirements; (2) effectiveness of information security controls; and (3) overall impact of an organization's information security program. Experts and leading organizations also identified four key attributes of successful measures. Specifically, measures should be quantifiable, meaningful (i.e., have targets for tracking progress, be clearly defined, and be linked to organizational priorities), repeatable and consistent, and actionable (i.e., be able to be used to make decisions).

Practices of leading organizations for developing measures emphasized the importance of focusing on the risks facing the organization, involving stakeholders from the beginning of the development process, assigning accountability for results, and linking information security programs to overall business goals. Key practices for using the resulting measurements include tailoring information to specific audiences (e.g., senior executives or unit managers); correlating measures to better assess outcomes; and reporting on the progress, trends, and weaknesses revealed by the collected data.

Federal agencies have tended to rely on compliance measures for evaluating their information security controls and programs. The measures developed by agencies have not always exhibited the key attributes identified by leading organizations, and agencies have not always followed key practices in developing their measures, such as focusing on risks. To the extent that agencies do not measure the effectiveness and impact of their information security activities, they may be unable to determine whether their information security programs are meeting their goals.

OMB's process for collecting and reporting on agency information security programs employs key practices identified by leading organizations and experts but is lacking in some areas. Specifically, many of the measures that OMB requires have key attributes such as being quantifiable, having targets, and being repeatable and consistent, but others do not. Further, OMB's process for collecting information from agencies relies on measures that do not demonstrate the effectiveness of control activities or the impact of information security programs. In addition, OMB does not adequately tailor its reporting for its congressional audience, correlate the data it collects, or discuss trends and weaknesses in information security controls and programs. Until OMB collects measures of the effectiveness of information security programs and appropriately reports the results, Congress will be hindered in its assessment of federal agencies' information security programs.