United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Thursday, October 29, 2009

INFORMATION SECURITY

Concerted Effort Needed to Improve Federal Performance Measures

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-10-159T

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on how agencies can establish cost-effective cyber defense. My statement today is based on our report titled *Information Security: Concerted Effort Needed to Improve Federal Performance Measures,* which is being released at this hearing.[1]

Cyber security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. Organizations are faced with a variety of information security threats, such as fraudulent activity from cyber criminals, unauthorized access by disgruntled or dishonest employees, and denial-of-service attacks and other disruptions. The recent dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology all contribute to the urgency of ensuring that adequate steps are taken to protect the federal government's information and the systems that contain and process it.

The Federal Information Security Management Act (FISMA), which was enacted in 2002, sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. The act assigns specific responsibilities to federal agencies, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). It also requires agencies and OMB to annually report on the adequacy and effectiveness of agency information security programs and compliance with the provisions of the act. To help meet these requirements, OMB established a uniform set of information security measures that all federal agencies report on annually.

Mr. Chairman, in light of questions about whether or not agencies are measuring the right things in securing their systems, you requested that GAO examine how organizations develop and use

[1]GAO-09-617 (Washington, D.C.: Sept. 14, 2009).

metrics to assess the performance and effectiveness of information security activities. In response to your request, our report and my statement provide (1) a description of key types and attributes of performance measures; (2) information about the practices of leading organizations for developing and using measures to guide and monitor information security control activities;[2] (3) information on the measures used by federal agencies to guide and monitor information security control activities and how they are developed; and (4) an assessment of the effectiveness of the measures-reporting practices that the federal government uses to inform Congress on the effectiveness of information security programs. In conducting this work, we collected and analyzed information from leading organizations, security experts, NIST, 24 major federal agencies, and OMB.[3] Our work for this report was performed in accordance with generally accepted government auditing standards.

In brief, Mr. Chairman, leading organizations and experts have identified different types of measures that are useful in helping to achieve information security goals. While officials categorized these types using varying terminology, we concluded that they generally fell into three types: (1) compliance, (2) control effectiveness, and (3) program impact. These types are consistent with those laid out by NIST in its information security performance measurement guide.[4] In addition, while information security measures can be grouped into these three major types, organizations and experts reported that all such measures generally have certain key characteristics, or attributes. These attributes include being (1)

[2]For the purposes of this report, "leading organizations" refers to prominent, nationally known organizations, academic institutions, and state agencies that have implemented comprehensive enterprisewide information security programs.

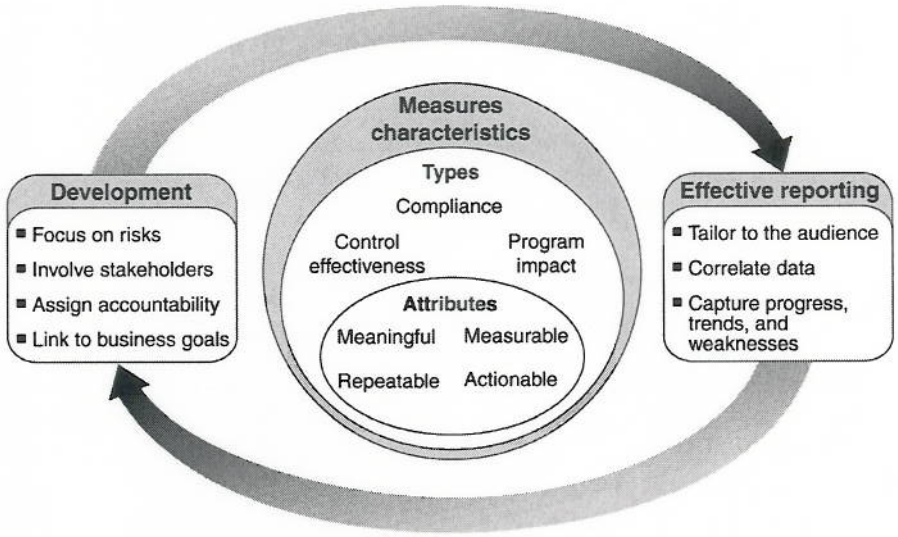
[3]The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

[4] National Institute of Standards and Technology, *Performance Measurement Guide for Information Security*, NIST Special Pub. 800-55 Revision 1 (Gaithersburg, Md.: July 2008).

measurable, (2) meaningful, (3) repeatable and consistent, and (4) actionable.[5]

Further, these organizations and experts indicated that the successful development of information security measures depends on adherence to a number of key practices, including focusing on risks, involving stakeholders, assigning accountability, and linking to business goals. Additional practices are critical to ensuring that the measures are useful in effectively conveying information to operational managers, executives, and oversight officials. These include tailoring measures to the audience; correlating data; and capturing progress, trends, and weaknesses. Figure 1 illustrates the interrelationship of these key practices with the key characteristics.

Figure1: Measures Development and Use Cycle



Source: GAO.

[5] Although we focused on identifying attributes and practices for measuring the performance of information security programs, our findings conformed closely to our prior work on effective performance measurement and reporting practices for the federal government in general. See, for example, GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making,* GAO-05-927 (Washington, D.C.: Sept. 9, 2005).

We determined that federal agencies have not always followed key practices identified by leading organizations for developing information security performance measures. While agencies have developed measures that fall into each of the three major types (i.e. compliance, control effectiveness, and program impact), on balance they have relied primarily on compliance measures, which have a limited ability to gauge program effectiveness. Agencies stated that, for the most part, they predominantly collected measures of compliance because they were focused on measures associated with OMB's FISMA reporting requirements. In addition, while most agencies have developed some measures that include the four key attributes identified by leading organizations and experts, these attributes were not always present in all agency measures. Further, agencies have not always followed key practices in developing measures, such as focusing on risks.

Lastly, we determined that OMB's measures did not address the effectiveness of several key areas of information security controls, including, for example, agency security control testing and evaluation processes. There is no measure of the quality of agencies' test and evaluation processes or results that demonstrate the effectiveness of the controls that were evaluated. [6] In addition, OMB's report to Congress does not fully employ key practices for reporting and thus provides limited information about the effectiveness of agency information security programs.

We made five recommendations to OMB to assist federal agencies in developing and using measures that better address the effectiveness of their information security programs:

- issue revised guidance to chief information officers for developing measures;

[6] OMB does require agency inspectors general to assess agencies' certification and accreditation process; however, the assessment may or may not include an assessment of security control testing and evaluation processes. Further, OMB does not provide a transparent depiction of how an assessment of an agency's security control testing and evaluation process contributes to the overall certification and accreditation quality rating.

- direct chief information officers to ensure that measures exhibit key attributes;
- direct chief information officers to employ the key practices for developing a measure as identified by leading organizations;
- revise annual FISMA reporting guidance to agencies; and
- revise the annual FISMA report to Congress to provide better status information on the security posture of the federal government.

Implementing these recommendations will help to focus attention on activities that will enhance the effectiveness of agency information security controls and improve the cyber defense of federal computer systems and information. In providing oral comments on a draft of the report, representatives of OMB's Office of E-Government and Information Technology stated that they generally agreed with the contents and recommendations of the report.

Mr. Chairman, this concludes my prepared statement. I would be pleased to respond to any questions that you or other members of the subcommittee may have.

For questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Individuals making key contributors to this testimony include Ashley Brooks, John de Ferrari, Season Dietrich, Neil Doherty, Ronalynn Espedido, Min Hyun, Anjalique Lawrence, Joshua Leiling, Lee McCracken, and David Plocher.