

GAO

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

September 2009

INFORMATION SECURITY

Concerted Effort Needed to Improve Federal Performance Measures



GAO

Accountability * Integrity * Reliability



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 wilshusen@gao.gov.

INFORMATION SECURITY

Concerted Effort Needed to Improve Federal Performance Measures

What GAO Found

Experts and leading organizations (nationally known organizations, academic institutions, and state agencies with enterprise-wide 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.

Contents

Letter		1
	Background	2
	Leading Organizations and Experts Identified Key Types and Attributes of Information Security Measures	7
	Leading Organizations and Experts Identified Key Practices for Developing and Using Information Security Measures	12
	Agency Information Security Measures and Development Processes Have Not Always Fully Adhered to Key Practices	18
	Measures in Annual FISMA Reports Have Not Captured the Effectiveness of Federal Information Security Programs	27
	Conclusions	36
	Recommendations for Executive Action	37
	Agency Comments	38
Appendix I	Objectives, Scope, and Methodology	39
Appendix II	References on Information Security Measures	41
Appendix III	GAO Contact and Staff Acknowledgments	44
Table		
	Table 1: References on Information Security Performance Measures	41
Figures		
	Figure 1: Measures Development and Use Cycle	13
	Figure 2: Types of Information Security Measures	19
	Figure 3: Attributes of Effective Measures	21
	Figure 4: Practices Essential in Developing Measures	24
	Figure 5: Measurement Types	28
	Figure 6: Attributes of Measures	30
	Figure 7: Effective Reporting of Measures	34

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act of 2002
GPRA	Government Performance and Results Act of 1993
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 14, 2009

The Honorable Tom R. Carper
Chairman
Subcommittee on Federal Financial Management, Government
Information, Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Mr. Chairman:

Information 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.

Information security performance measures (also called metrics) are used to help determine whether an agency is achieving its information security goals. Over the past several years, major federal agencies have consistently reported progress in performing certain information security control activities, and they have used a variety of measures as the basis for their conclusions regarding their progress.

In this regard, you asked us to examine how organizations develop and use measures to assess the performance and effectiveness of information security activities. In response to your request, our objectives were to (1) describe key types and attributes of performance measures, (2) identify the practices of leading organizations for developing and using measures to guide and monitor information security control activities,¹ (3) identify

¹For the purposes of this review, "leading organizations" refers to prominent, nationally known organizations, academic institutions, and state agencies that have implemented comprehensive enterprisewide information security programs.

the measures used by federal agencies to guide and monitor information security control activities and how they are developed, and (4) assess the effectiveness of the measures-reporting practices that the federal government uses to inform Congress on the effectiveness of information security programs.

To identify key types and attributes of performance measures, we collected and analyzed information from leading organizations, security experts, and the National Institute of Standards and Technology (NIST). To identify practices of leading organizations, we obtained information primarily through interviews with senior officials and document analysis conducted during and after visits to the 14 organizations we studied. We supplemented the information gathered from organizations with information obtained from four information security experts. To identify measures used and developed by federal agencies, we collected and analyzed agency-specific information about measures, policies, plans, and practices. To determine the effectiveness of reporting practices, we reviewed prior GAO reports and relevant laws and guidance such as the Federal Information Security Management Act of 2002 (FISMA) to identify mandatory and optional practices for reporting information security program information (including performance measurement information) to the Office of Management and Budget (OMB) and Congress.

We conducted this performance audit from July 2008 through September 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I contains additional details on the objectives, scope, and methodology of our review.

Background

Performance measures can be used to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements. Such measures can be used to monitor the accomplishment of goals and objectives and analyze the adequacy of control activities. Thus, performance measures should provide managers and other stakeholders with timely, action-oriented information in a format that facilitates decisions aimed at improving program performance.

Measuring performance allows organizations to track the progress they are making toward their goals and gives managers crucial information on which to base their organizational and management decisions. Performance measures can also create powerful incentives to influence organizational and individual behavior.

Federal Agencies Are Required to Measure and Report on Program Performance

Performance measures, including information security measures, are a key element in the performance management approach to implementing federal programs. The Government Performance and Results Act of 1993 (GPRA) established a statutory framework for performance management and accountability within the federal government. GPRA introduced planning and reporting requirements that sought to shift the focus of federal management and decision making from a preoccupation with the number of program tasks or activities completed or services provided to a more direct consideration of the results of programs. The act was intended to improve federal program effectiveness, accountability, and service delivery. It requires federal agencies to develop both long- and near-term outcome-oriented goals, to describe how they will measure progress toward the achievement of those goals in annual performance plans, and to report annually on their progress in program performance reports.

GPRA incorporates performance measurement as one of its most important features. In reviewing performance measures shortly after GPRA was enacted, we found that agencies that were successful in adopting performance measures ensured that the measures (1) were tied to program goals and demonstrated the degree to which the desired results were achieved, (2) were limited to a vital few that were considered essential for producing data for decision making, (3) covered multiple priorities, and (4) provided useful information for decision making.² However, despite having more performance measures available, federal managers' reported use of performance information in management decision making has not changed significantly. We have previously reported practices that can facilitate using performance information for decision making. For example, to ensure that performance information will be both useful and used in decision making throughout the organization, agencies need to consider users' differing policy and

²GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1, 1996).

management information needs. Practices that improve the usefulness of performance information can help to meet those needs.

Performance planning and measurement have slowly yet increasingly become a part of agencies' cultures.³ According to three governmentwide, random sample surveys of federal managers that we conducted in 1997, 2000, and 2003, managers reported having significantly more of the types of performance measures called for by GPRA, particularly outcome-oriented performance measures, in 2003 than in 1997, when GPRA went into effect governmentwide.

Agencies' Annual Reporting on Information Security Includes Performance Measures

The Federal Information Security Management Act (FISMA), which was enacted in 2002 as part of the E-Government Act, sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. FISMA's framework is based on a cycle of risk management activities necessary for an effective security program, such as assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. In order to ensure the implementation of this framework, the act assigns specific responsibilities to agencies, OMB, and NIST.

FISMA requires agencies to implement information security programs that include such things as periodic assessments of risk; risk-based policies and procedures; security awareness training; and procedures for detecting, reporting, and responding to security incidents. Further, FISMA also requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General of the United States on the adequacy of its information security policies, procedures, practices, and compliance with requirements.

FISMA also requires agencies to have independent evaluations of their information security programs conducted on an annual basis by the agency Inspector General or an independent external auditor. These evaluations are to include testing of the effectiveness of the information security policies, procedures, and practices of a representative subset of

³GAO, *Managing For Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-927 (Washington, D.C.: Sept. 9, 2005).

the agency's information systems as well as an assessment of compliance with the requirements of the act.

FISMA states that the director of OMB shall oversee agency information security policies and practices including, among other things, overseeing agency compliance with FISMA to enforce accountability, and reviewing at least annually and approving or disapproving agency information security programs. In addition, the act requires that OMB report to Congress no later than March 1 of each year on agency compliance with FISMA.

To meet its requirements, OMB requires federal agencies to annually report on information security, and sets forth its requirements for meeting these provisions in annual reporting instructions to agencies. The instructions require agencies to provide information with regard to, among other things, certification and accreditation, security awareness training, incident response, and configuration management. Beginning in 2007, OMB has also required agencies to provide information on measures related to the effectiveness of their security policies and procedures. In all, OMB has established a uniform set of 24 measures of information security programs that all federal agencies report on annually.

OMB uses the information submitted by agencies as well as a summary of the findings of independent evaluations in its overall evaluation of federal information security performance. In its report to Congress, OMB is to identify significant deficiencies in agency information security practices as well as planned remedial actions to address such deficiencies. OMB's 2008 report to Congress provided information on the federal government's progress in meeting key security performance measures from fiscal year 2002 through 2008, an assessment of governmentwide information technology (IT) security strengths and weaknesses, and a plan of action to improve performance. Additionally, agency Inspectors General were asked to provide information on the quality of agency plans of action, milestone processes, and certification and accreditation processes, as well as assessments of the completeness of agency systems inventories.

Under FISMA, NIST is tasked with developing standards to be used by agencies to categorize their information and systems, based on the objectives of providing appropriate levels of information security according to a range of risk levels, as well as minimum information security requirements for information and systems in each category. In July 2008, NIST published its *Performance Measurement Guide for Information Security* to assist agencies in the development, selection, and

implementation of information system-level and program-level measures.⁴ The guide describes how an organization, through the use of measures, can identify the adequacy of in-place security controls, policies, and procedures. The guide also provides an underlying data collection, analysis, and reporting infrastructure that can be tailored to support FISMA performance measures. OMB requires agencies to follow NIST guidance in implementing their information security programs, and thus agencies are required to follow the practices in the NIST performance measurement guide.

We Have Previously Made Recommendations for Improving Reporting on FISMA Implementation

We have previously reported that despite federal agencies' reported progress and increased security-related activities, weaknesses remained in the processes they used for implementing FISMA. In addition, we have also identified a need to improve the use of performance measures to assist agencies in FISMA implementation and have made recommendations to OMB on its annual reporting instructions to agencies:

- In 2005, 2006, and 2007, we recommended that OMB improve FISMA reporting by clarifying reporting instructions and requesting agency Inspectors General to report on the quality of additional agency processes, such as the annual system reviews, system test and evaluation, risk categorization, security awareness training, and incident reporting.⁵
- Additionally, in 2007 we recommended that OMB develop additional performance measures that gauge the effectiveness of FISMA activities.⁶

OMB agreed to take our recommendations under advisement when modifying its FISMA reporting instructions for subsequent years.

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

⁵GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, [GAO-05-552](#) (Washington, D.C.: July 15, 2005); *Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, [GAO-07-65](#) (Washington, D.C.: Oct. 20, 2006); and *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, [GAO-07-837](#) (Washington, D.C.: July 27, 2007).

⁶[GAO-07-837](#).

Leading Organizations and Experts Identified Key Types and Attributes of Information Security Measures

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 categories: (1) compliance, (2) effectiveness of controls, and (3) program impact. These three categories are consistent with those laid out by NIST in its information security performance measurement guide, which serves as official guidance on information security measures for federal agencies and which OMB requires agencies to follow.

Compliance

Leading organizations developed compliance measures to determine the extent to which security controls were in place that adhered to internal policies, industry standards, or other legal or regulatory requirements. NIST guidance refers to these as implementation measures because they focus on measuring progress in implementing security programs, specific security controls, and associated policies and procedures. These measures are effective at pointing out where improvements are needed in implementing required policies and procedures. However, they provide only limited insight into the overall performance of an organization's information security program.

As an example, a state organization reported that it was subject to a variety of specific requirements concerning the structure of its information security program. To demonstrate compliance with these requirements, the organization reported that it used measures such as whether quarterly updates were made to corrective action plans and whether an information security officer had been designated within a specified number of years. Another organization reported that it was subject to an industry regulation requiring managers to complete reviews of applications for employee access rights. To measure compliance with this regulation, the organization established a metric that identified the percentage of managers who had completed such reviews.

Control Effectiveness

Control effectiveness measures go beyond compliance measures to characterize the extent to which specific control activities within an organization's information security program meet their objectives. Rather than merely capturing what controls are in place, such measures gauge how effectively the controls have been implemented. These types of measures can show such things as how well an organization responds to

security events or the likelihood that known vulnerabilities will be exploited. According to NIST, such measures concentrate on the evidence and results of assessments and may require multiple data points quantifying the degree to which information security controls are implemented and the resulting effect on an organization's information security posture. Leading organizations and experts agreed that control effectiveness measures are more advanced than compliance measures because they characterize the performance of controls rather than merely indicating the extent to which such controls are in place.

One type of effectiveness measure uses tests to measure how effectively an organization responds to a security challenge. For example, to determine whether users had adopted effective security practices as a result of training, a manufacturer and an academic institution tested such things as the extent to which controlled e-mail phishing schemes were successful and the strength of passwords that users had chosen.⁷ Another type of effectiveness measure addresses the timeliness with which security control activities are performed. For example, a telecommunications organization developed measures such as *percentage of (high/medium) vulnerabilities closed within 90 days* and *percentage of systems patched within 30 days* to measure the effectiveness of its patch and vulnerability management controls. In these examples, prompt abatement of vulnerabilities and patching of systems were interpreted as indications that implementation of these controls was highly effective.

In another example of effectiveness measures, several leading organizations measured the effectiveness of their security awareness training by measuring the material covered and timing of training and comparing it with the occurrence of security incidents. A change in the number of security incidents occurred after training had been conducted was taken as an indication of the effectiveness of the training.

Program Impact

Program impact measures are similar to but broader and more all-encompassing than control effectiveness measures. Rather than focusing on the effectiveness of specific control activities, program impact measures gauge the overall outcome of an organization's information

⁷Phishing is tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

security program in mitigating security risks. Leading organizations and experts pointed out that program impact measures could be developed by analyzing the relationships among other measures to derive a measure of the overall impact of various control activities on the organization's risk profile. For example, individual measures, including control effectiveness measures that offer insight into specific information security controls, could be correlated to develop a program impact measure. Other program impact measures could allow managers and decision makers to gauge overall progress of an information security program over time in achieving its objectives. NIST points out that this broader view also requires that impact measures include information about the resources invested in an information security program so that insight into the value of information security to the organization can be gained. Because impact measures are built on a program with other measures already well established, they are the most advanced of the three major measures types.

An example of an impact metric involves a financial institution that wanted to better understand its malware risks.⁸ To do so, the institution developed a metric that compared a compliance metric (*percentage of systems with updated antivirus software*) with a control effectiveness metric (*time [number of hours] to deploy new patches [from a security vendor] to all systems*) to produce a measure of the organization's overall exposure to malware because of systems not being fully up to date with security patches. The institution found that the measure could be used to gauge the overall impact of its information security program on the risk of malware infection.

Useful Measures Exhibit Four Key Attributes

While information security measures can be grouped into these three major types, organizations and experts we contacted reported that all such measures generally have certain key characteristics, or attributes. These attributes include being (1) measurable, (2) meaningful, (3) repeatable and consistent, and (4) actionable.⁹

⁸Malware (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded in useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.

⁹Although 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-05-927](#).

Measurable

The organizations we studied reported that they aimed to establish measures that could be expressed in *quantifiable* values. Quantitative measures, such as numbers and percentages, assign value to measurement data and can be used to facilitate comparison with other information. Thus it is possible to make adjustments to control activities to better achieve information security objectives. For instance, a telecommunications organization in our study based its high-level, qualitative measure (e.g., red, yellow, or green) for patching controls on quantitative operational measures, such as *percentage of systems patched within 30 days*. Such a metric allowed the organization to determine whether its goal for software patching had been achieved by comparing actual results with performance benchmarks and projections.

Meaningful

Leading organizations and experts stated that measures were most *meaningful* to an organization when they (1) had targets or thresholds for each measure to track progress over time; (2) were clearly defined to precisely reflect what was being measured; and (3) were linked to organizational priorities, such as quality, timeliness, or best use of available resources. In other words, meaningful measures are relevant and consequential to an organization's goals. The example previously mentioned of the telecommunications organization's metric of *percentage of systems patched within 30 days* is a good example of a measure with a specific target that can provide a meaningful indication of the responsiveness of an organization's information security program. In another example, a manufacturing organization stated that it had been challenged to clearly define measures that had been obscured by the use of technical jargon. To address this challenge, the organization developed a catalog with a clear definition for each metric. Another organization, a large defense contractor, reported that it took steps to link its measures to organizational priorities. For example, having established timeliness and responsiveness as priorities, the organization implemented measures such as *time between compromise and detection*—the average amount of time it took for its information security personnel to detect a security incident once it had occurred. Thus, the contractor used a clearly defined metric to address an organizational priority—responding quickly to any compromise of its networks.

Repeatable and Consistent

Organizations developed measures that were *repeatable* and produced *consistent* results by ensuring that the measures were defensible, were auditable, used readily obtainable data, and could be easily reproduced. Repeatable measures are the result of a measurement process that is implemented consistently over time to ensure that measurements are comparable with each other. For example, a security services provider ensured consistency by developing a process around measures that required data inputs to follow a common enterprise reporting mechanism. According to IT security staff, the consistently implemented measurement process helped to reduce the likelihood that the results would be misinterpreted because of variations in how measures had been reported over time. Likewise, a financial institution reported that it had a policy of only developing measures around business processes that had proven to be repeatable.

Actionable

Organizations also aimed to develop measures that were *actionable* so that they could be used to make decisions about improving information security. According to leading organizations and experts, actionable measures support the decision-making process and drive the behavior of those who are responsible for the control activities reflected in the measures. Such measures provide specific indications about aspects of the information security program so that adjustments can be made by responsible officials. For example, a financial institution developed measures linked to the effectiveness of its access controls. One of the priorities of the organization was to closely monitor and control access privileges granted to employees, which it did primarily through periodic reviews of such privileges. To drive the behavior of those accountable for this activity, the organization developed measures such as *percentage of reviews completed* and *number of reviews past due*, which link closely to the organization's control objectives. Highlighting the extent to which these actions had been taken provides a basis for managers to hold staff accountable for ensuring that reviews were performed on a timely basis.

These attributes are consistent with those laid out by NIST in its information security performance measurement guide.¹⁰ For example, NIST notes that

- measures must yield quantifiable information (percentages, averages, and numbers);
- data supporting measures need to be readily obtainable and feasible to measure, in order to provide meaningful data;
- only repeatable information security processes should be considered for measurement; and
- measures must be useful for tracking performance and directing resources.

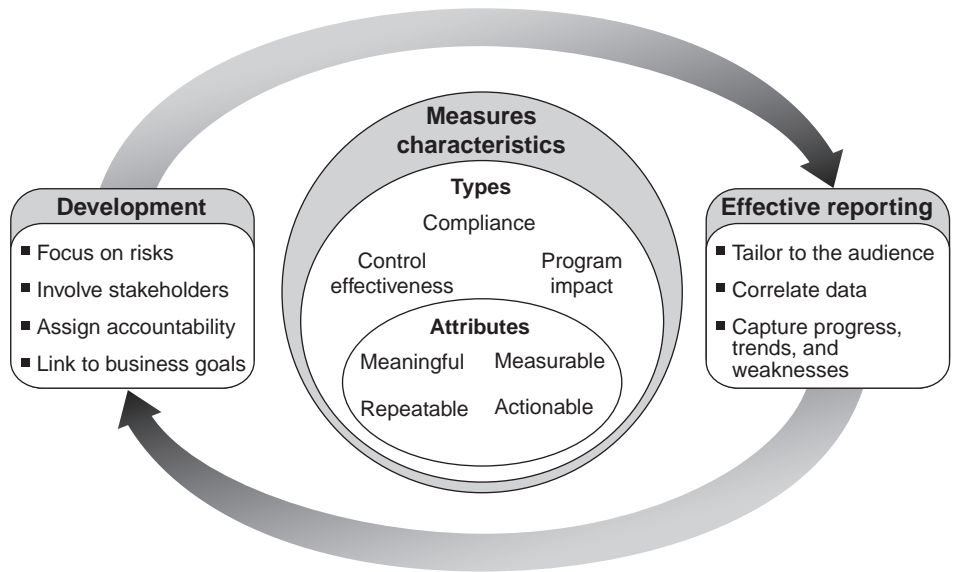
To illustrate examples of effective performance measures, the NIST guidance provides examples with structured descriptions in a template format. The template format facilitates presenting clear and consistent definitions for the measures.

Leading Organizations and Experts Identified Key Practices for Developing and Using Information Security Measures

Leading organizations and experts from whom we obtained input 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 previously discussed.

¹⁰NIST, Special Publication 800-55.

Figure 1: Measures Development and Use Cycle



Source: GAO.

While different organizations and experts had varying terms for these items and prioritized them in different ways, they generally identified these as important factors in effectively developing and using information security measures.

Leading Organizations Develop and Use Measures That Span All Major Types and Have All Key Attributes

Leading organizations and experts stressed that it was important to develop and use different types of measures to ensure that the measurement process is comprehensive and useful in helping them achieve their information security goals. Specifically, they indicated that all three types of measures should be used to ensure that the performance of the information security program can be fully assessed. For example, a performance measurement process that only considers compliance with standardized procedures and rules will not be able to provide insight into how effective the controls are or whether the program is achieving its objectives.

Control effectiveness measures can provide insight into effectiveness beyond what is possible with compliance measures alone. However, program impact measures are also needed to provide a broader perspective on the success of the information security program as a whole. NIST’s guidance notes that the most mature programs use both

effectiveness measures and program impact measures to determine the effect of their information security processes and procedures.

In Developing Measures, Leading Organizations Focus on Risks, Involve Stakeholders, Assign Accountability, and Link to Business Goals

In developing information security measures, leading organizations—as well as information security experts we consulted—identified a number of key practices that they considered essential to ensuring that such measures are useful for monitoring and guiding information security control activities. While different organizations and experts have focused on different aspects of developing useful measures, they generally agreed that the following four practices are key.

Focus on Risks

Leading organizations generally employed a risk-based approach for developing measures. Such an approach recognizes that security risks can never be completely eliminated and that resource constraints also inevitably limit the extent to which controls can be implemented. The risk-based approach attempts to ensure that risks to the organization are identified and prioritized so that available resources can be most effectively spent in defending against the most significant threats, such as successful attack techniques, for instance. Further, since risks change over time, leading organizations reported that they periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected to mitigate those risks. Because information security controls are to be tailored to address identified risks, measures likewise can be most useful when they are also keyed to these same risks and controls. Focusing on risks is also consistent with developing measures that are meaningful and actionable, as discussed in the previous section and as the following examples illustrate:

- An academic institution used NIST’s risk assessment framework to determine enterprise risks and where information security efforts needed to be focused. Then it developed security measures that were linked to these priorities so that it could determine how well it was mitigating risks.
- A financial institution developed measures focused on measuring the performance of controls designed to mitigate priority operational risks. For example, the institution identified software vulnerabilities as a priority risk and established targets for patching such vulnerabilities promptly. By collecting measures that indicated how quickly its systems were patched, the organization was able to focus attention on meeting its performance targets and mitigating the priority risk.

-
- A manufacturing corporation used security measures to identify emerging security threats as the most significant risk it faced and, in response, undertook a proactive approach toward preventing potential security incidents from occurring. For instance, by looking at the *number of virus detections over time*, the corporation believes it can identify a particular pattern or anomaly that could provide insights useful in detecting a newer trend in the threat environment.

Involve Stakeholders

In developing risk-based measures, leading organizations and security experts recommended that organizations identify key stakeholders and secure their involvement from the inception of the measures development process to ensure that the process is fully supported throughout the organization, is linked to key business processes, and can be used to drive behavior. For instance, at one university, key stakeholders—including the Chief Information Officer, Chief Technology Officer, and Chief Information Security Officer—were involved in the development of information security measures because of their critical role in driving behavior within the organization. Likewise, a financial organization stressed that in order for a measures program to demonstrate continued progress, senior leadership involvement was critical from the onset. A subject matter expert also noted the importance of involving senior management to understand and accept the risks and support the implementation of information security activities throughout an organization. NIST, in its guidance, also asserts that an effective risk management program requires the support and involvement of senior management and notes the importance of involving stakeholders in every step of the measures development process to ensure organizational support.

Assign Accountability

In addition to involving key stakeholders, leading organizations also tended to identify “owners” for the control activities gauged by specific security measures. These individuals were to be responsible and accountable for the effective implementation of the control activities reflected in specific measures. For example, a financial institution held measures owners (e.g., operational managers, system owners, or project managers) accountable for results. Specifically, these owners had to ensure that their business units had compliance levels of 95 percent or higher. Another organization, a global services contractor, held individual

managers responsible for each metric and considered the performance of the control activities reflected in the measures when making promotion decisions.

Experts also noted that security measures should have owners at the management level who are held accountable through performance appraisals that can be affected by the results of the measures. They emphasized the importance of metric ownership to the success of the measures program and noted that this practice is common in industries such as finance, manufacturing, and health care.

Link to Business Goals

Leading organizations reported that in developing their information security programs, they worked to ensure that their security measures were linked, at some level, to the organization's overall business goals. They noted that information security needs to be explicitly tied to at least one goal or objective in the strategic planning process to demonstrate its importance in accomplishing the organization's mission. This connection can be established by identifying business goals and objectives that drive the implementation of information security controls. Our previous work concluded that assessing information security risks in terms of the impact on business operations was an essential step in determining what controls were needed and what level of resources should be expended on controls.¹¹ As discussed in the previous section, the development of program impact measures goes a long way toward ensuring that measures are linked to business goals.

NIST likewise states that when determining which measures to develop, goals and objectives from policies, guidance, and regulations should be identified and prioritized to ensure that the measurable aspects of information security performance correspond to the operational priorities of the organization.

¹¹GAO, *Executive Guide: Information Security Management—Learning From Leading Organizations*, AIMD-98-68 (Washington, D.C.: May 1, 1998).

Leading Organizations Advocate Key Practices for Using Measures to Communicate about Information Security

Effective use of information security measures is a key element in communicating about the progress and success of an information security program. Effective use of measures highlights achievements as well as areas for improvement, demonstrates management’s commitment to information security, and can drive behavior to better achieve program objectives. Leading organizations—as well as information security experts we consulted—identified the following three practices as key to effective use of measures.

Tailor to the Audience

Organizations generally agreed that when communicating about measures, a key consideration is the intended audience. Measures can vary in scope and purpose. At the lowest level, organizations may have large numbers of narrowly defined measures corresponding to the implementation of specific control activities. Presenting these may be appropriate for information security managers but not for higher-level executives. Similarly, program impact measures derived from lower-level measures may be meaningful for top management and oversight officials but not very actionable when presented to lower-level information security officials. Thus the most effective communications are likely to result from tailoring measures presentations to the needs of the intended audience. For example, at a large financial institution the measurement report provided to senior executives is a one-page summary of selected programs, accomplishments, major issues or risks, and the status of measures related to them. The report sent to unit managers is more detailed and includes in-depth measures of the current status, historical trends, and future outlook of specific control activities. At a state organization, measures reported annually to the Governor and a finance committee are focused on an overview of the state’s security posture. However, monthly measurement reports to the Governor’s homeland security office focus in more detail on threats to the state’s network. Officials noted that these reports have allowed each audience to make strategic security decisions, formulate action plans, and identify areas where additional attention needs to be focused.

Correlate Data

Just as certain measures—program impact measures as well as some control effectiveness measures—can be created by linking lower-level measures, so useful higher-level presentations about measures depend on appropriately correlating available measures data. When reporting measures to executives and other decision makers, leading organizations

and security experts recommended correlating the data from multiple individual measures to present more meaningful information. Correlated measures can be based on multiple measurement types (e.g., compliance and effectiveness measures) and can provide insight into the effectiveness of security controls and programs within an organization. For instance, one state organization reported on a measure of its overall security posture that was compiled according to a standard formula from multiple lower-level measures. Another organization compared the findings of audit and risk assessments with their associated compliance measures to determine the extent of systemic issues in a particular area.

Capture Progress, Trends, and Weaknesses

In addition to correlating data, leading organizations have structured their communications about information security measures to include data on progress, trends, and weaknesses or deficiencies of information security controls. Including trend data illustrates improved or declining performance by comparing data points over time, an important reason why measures need to be repeatable, as discussed in the previous section. At a state-run organization, the information security measures report included a network threat graph that showed the number of times the incident response team had been activated to respond to attacks on the state network, by month. Another chart showed trends in the number of security audits conducted each year. At a financial institution, for various measures, the report provided a 12-month history of its performance, highlighting current, historical, and future trends.

Agency Information Security Measures and Development Processes Have Not Always Fully Adhered to Key Practices

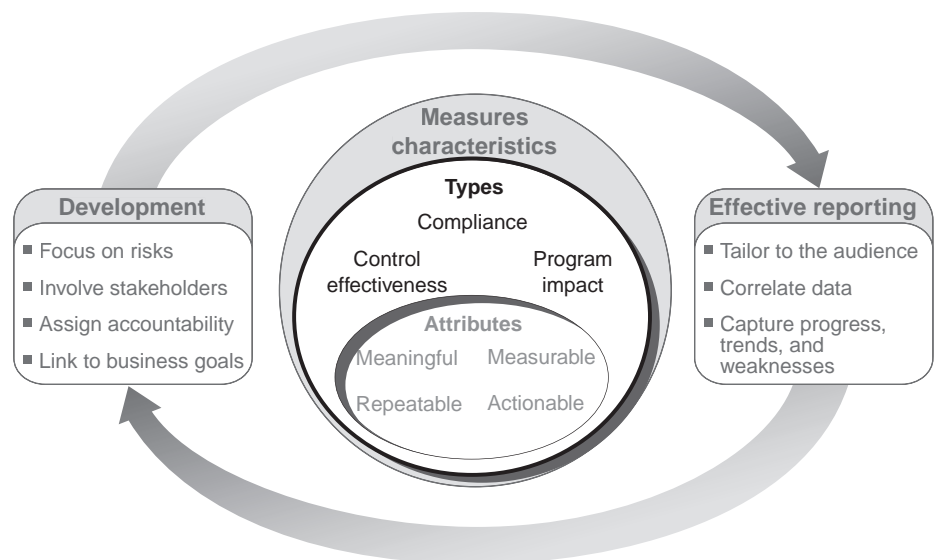
Federal agencies' information security performance measures and their processes for developing them have not always followed key practices identified by leading organizations. While agencies have developed measures that fall into each of the three major types (i.e., compliance, control effectiveness, and program impact), on balance they have relied primarily on compliance measures, which have a limited ability to gauge program effectiveness. In addition, while most agencies have developed measures that include the four key attributes identified by leading organizations and experts, these attributes are not always present in all agency measures. Further, agencies often have not always followed key practices in developing their metrics. Few were focused directly on mitigating the greatest risks, though the majority of agencies reported involving key stakeholders in the development process as well as assigning individual responsibility for control activities gauged by specific

measures. Information security measures also have not been explicitly aligned with agency business goals.

Agencies Primarily Use Compliance Measures to Assess Their Information Security Posture

Leading organizations noted that information security measures need to span all three major types to ensure that the performance of an agency information security program has been sufficiently assessed (see fig. 2). Information security experts and NIST guidance indicated that organizations with increasingly effective information security programs should migrate from predominantly using compliance measures toward using a balance of compliance, control effectiveness, and program impact measures.

Figure 2: Types of Information Security Measures



Source: GAO.

Our review and analysis of the types of measures used by 24 major agencies showed that a number of agencies have begun implementing balanced programs that include a substantial number of effectiveness and

program impact measures.¹² Specifically, 5 agencies had effectiveness measures that accounted for 25 to 50 percent of their total number of measures, and 1 agency had program impact measures that accounted for over 25 percent of its total number of measures. However, a significant number of agencies were predominantly using compliance measures and not including a significant number of effectiveness or program impact measures. Nineteen agencies had effectiveness measures that constituted less than 25 percent of their total number of measures. Two agencies indicated not using effectiveness measures at all. Similarly, 16 agencies reported that they did not use program impact measures. Approximately half of the compliance measures used by agencies were based on the measures OMB specified in its annual FISMA reporting instructions. Although all 24 agencies also used measures beyond what is required by OMB, these additional measures were also primarily compliance measures.

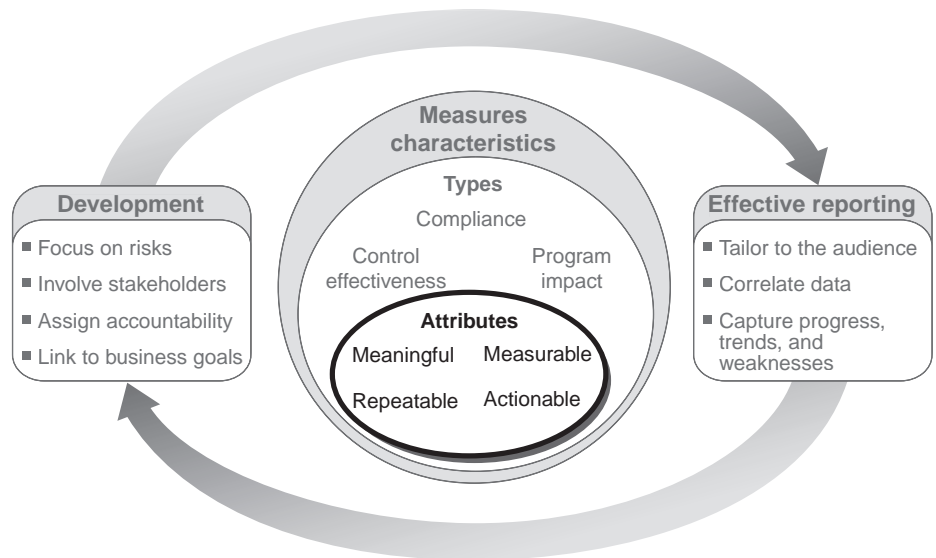
Agencies stated that, for the most part, they predominantly collected measures of compliance because they were focused on implementing measures associated with OMB's FISMA reporting requirements. As a result, agencies have been limited in the breadth and utility of the information they can provide based on their information security performance measures.

Agencies Have Not Always Implemented All Key Attributes of Effective Measures

As discussed earlier, key attributes or characteristics of measures include being (1) measurable, (2) meaningful, (3) repeatable and consistent, and (4) actionable (see fig. 3). Effective measures have all four attributes. Agency measures often embodied one or more of these attributes; however, the measures did not always address all key attributes.

¹²The 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. Total number of measures per agency varied from 4 to 100.

Figure 3: Attributes of Effective Measures



Source: GAO.

Not All Agencies Have Used Predominantly Quantitative Measures

Of the 24 agencies we surveyed, most, but not all, used predominantly quantitative measures. Specifically, 14 had discrete and quantitative measures comprising over 75 percent of their total number of measures, including 7 agencies for which 100 percent of their measures were quantitative. For an additional 7 agencies, 51 to 75 percent of their measures were quantitative. Examples of such measures included *percentage of incidents addressed according to policies* and *percentage of high-risk vulnerabilities mitigated in 30 days*. Such measures can be useful in comparing results with other information. However, for the remaining 3 agencies, less than half of their measures were quantitative. As an example of a nonquantitative measure, one agency reported its Trusted Internet Connections implementation approach as an outcome-based performance measure—intended to determine the effectiveness or efficiency of information security policies and procedures. The measure, however, did not include a discrete unit of measure, but solely a description of the agency’s plans to deploy *six Trusted Internet Connections access points* and its inclusion of *Internet portal consolidation alternatives, justifications, and significant milestones*. Another agency developed a measure for continuity of operations planning by measuring the extent to which the plan *enables the execution in a*

degraded environment or at alternate locations using qualitative indicators—such as “minor,” “some,” “significant,” and “major” deficiencies—that were not defined. Examples of other agency measures that could result in ambiguous results include *ensure systems have no default user IDs, review IT use policy document and update as necessary, and conduct reviews of IT security programs at [the agency’s] operating units*. To the extent that agencies do not use quantifiable measures of their security control activities, they may limit their ability to produce accurate and useful assessments of their information security programs.

Agencies Measures Were Not Always Clearly Defined or Did Not Always Have Specific Performance Targets

While many agency measures were clearly defined, they were not consistently so in all cases and did not always set specific performance targets. Of the 24 agencies, 16 had clear definitions measures for over 75 percent of their total number of measures. Examples for which agencies had clear definitions include *total percentage of critical patches deployed by [component]* and *average length of time (in hours) between an incident being reported and the incident being closed*. By implementing such measures, the agencies have established a basis for measuring their progress that reflects their priorities of timeliness and responsiveness. For 6 agencies, 50 to 75 percent of their measures were clearly defined. For the remaining 2 agencies, 50 percent or less of their measures qualified as clearly defined. In these cases, for example, agencies may have listed general terms such as “patch management,” “management of plan of actions and milestones,” or “annual vulnerability testing by independent contractors” as measures without more specifically defining how those subjects were to be measured. One agency provided a brief description of its annual testing process as a measure without describing any specific measurement indicators. Use of such items as measures could lead to inconsistent and unreliable assessments of agencies’ information security programs.

In addition, of the 24 major agencies, none had specified a performance target for each measure collected, and only 5 agencies had established targets for more than 50 percent of their measures. Without consistently establishing targets, agencies do not have a benchmark by which they can measure success or identify remedial action. Further, if the success of a measure cannot be determined, agencies may need to reconsider the value in collecting those measures or redefine the measures.

Agency Measures Were Usually but Not Always Repeatable or Applied Consistently

Agencies usually implemented quantitative measures that were repeatable and could be consistently implemented; however, they did not always do so. All agencies used repeatable measures as demonstrated in their FISMA reports, submitted annually since fiscal year 2002. In alignment with leading practices, certain FISMA reporting measures, such as the *percentage of incidents with tested contingency plans* and *percentage of systems with tested security controls*, have been implemented consistently over time and are comparable with each other. Additionally, 19 of the 24 agencies indicated using measures to capture trend data, which can identify security performance strengths and vulnerabilities through historical data comparison.

However, agencies also implemented measures that relied on the qualitative assessment of the individual evaluating the measure, which can undermine repeatability and consistency. For instance, one agency used qualitative terms such as “minor,” “some,” “significant,” and “major” for assessing deficiencies in certain security controls. Without further specificity in the definitions or a consistent methodology for evaluating these controls, such subjective measures may not be useful in determining progress over time in addressing this risk.

Agencies Have Implemented Actionable Measures

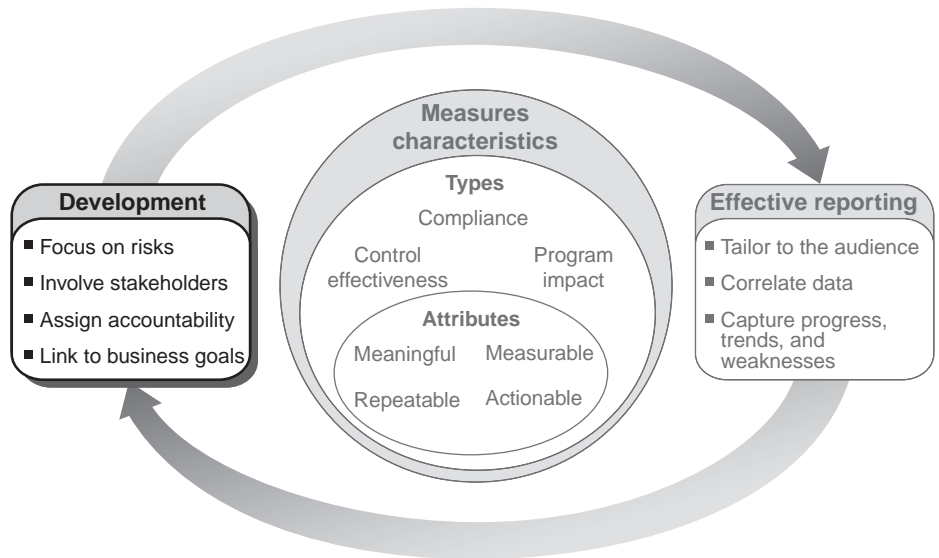
Most (22 of 24) agencies demonstrated that they have taken actions or made decisions based on the results of information security performance measures. For example, 1 agency had a practice of issuing memos to those sites that received a failing risk score based on metrics shown in monthly risk reports. The memos required that each site improve its risk score to a passing level within a specific period of time and offered additional resources to help reach this target. As another example, at 1 agency, users who were not logging off the network at the end of the day over the span of 3 months were identified and counseled on the security consequences associated with their actions, such as preventing the deployment of important security patches. The agency also committed to conducting periodic spot checks on these specific users to determine if additional action was required. In cases where measures were not actionable, agencies often collected status information, such as the number of personal identification verification cards issued or the number of systems granted an authority to operate. Such information is less likely to establish a meaningful basis upon which to take action.

While agencies in many cases have incorporated the key attributes of measures identified by leading organizations and experts, they are not consistently applying these attributes to all of the measures they develop and use. To the extent these attributes are not fully applied, agency measures may be limited in their usefulness in assessing the effectiveness of information security programs.

Agencies Did Not Always Employ Key Practices in Developing Measures

As previously discussed, leading organizations identified a number of key practices that are essential in developing measures to monitor an information security program (see fig. 4). According to our analysis of the information provided by the 24 major agencies, these key practices have not always been implemented.

Figure 4: Practices Essential in Developing Measures



Source: GAO.

Agency Measures Showed Limited Consideration of Risk

Leading organizations emphasized that risk is a key component in determining which measures to employ. Prioritizing measures based on the level of risk to the organization can enable agencies to undertake a proactive approach toward protecting their information and information systems and help preempt adverse outcomes (e.g., security incidents).

However, our review of agency measures showed that limited consideration was given to specific risks in developing performance measures. Further, very few (6 percent) of the measures collected were related to the risk assessment control activity itself, which includes conducting risk assessments, performing vulnerability scans, and categorizing security systems and the information they process. Additionally, while the certification and accreditation process includes performing risk assessments as a key step,¹³ the certification and accreditation measures that agencies used primarily focused on the percentage of systems certified and accredited, the percentage of systems with security controls tested, and/or the completion of corrective actions—all of which are compliance measures that do not discuss the effectiveness of those control activities in mitigating risks. By putting little emphasis on responding to specific risks, agencies may be missing opportunities to take a preemptive approach toward reducing their vulnerabilities in selecting their information security control activities. Moreover, agencies cannot demonstrate the effectiveness of their information security programs when they are not adequately considering risk.

Most Agencies Indicated That They Involved Key Stakeholders

NIST and experts recommended that organizations identify key stakeholders and obtain their involvement from the inception of the measures development process to ensure that key management and organizational priorities are reflected in the measures. Of the 24 major agencies, 19 indicated that they involved key stakeholders, including identifying the position of the individuals involved or a description of their specific roles and responsibilities associated with a measure. Five agencies did not mention stakeholder involvement in their measures development process. If stakeholders are omitted, agencies may not be providing key organizational decision makers with the measures they require to understand the effectiveness of information security performance within their domain.

¹³Certification and accreditation is the process of authorizing operation of a system, including the development and implementation of risk assessments and security controls.

Most Agencies Assigned Accountability for Measures to Individuals

In addition to involving key stakeholders, leading organizations also tended to identify owners, who were to be responsible and accountable for the effective implementation of the control activities reflected in specific measures. Twenty-one agencies indicated that they designated such owners. For instance, at one agency, if the owner identified a negative trend in a particular performance measure, he or she was responsible for taking the appropriate action to improve the particular process or activity that was negatively affecting the measure. Another agency assigned responsibility for a measure to the system owner at a particular site. Additionally, experts also noted that security measures should have owners at the management level, who are held accountable through performance appraisals that can be affected by the results of the measures. However, nearly half of the 24 agencies indicated that senior-level managers were consequently not held accountable. Some agencies assigned responsibility to information system owners or specific individuals and did not indicate senior-level manager ownership of measures. In doing so, agencies are forgoing a practice that experts have said can play a key role in ensuring the success of a metrics program.

Agency Measures Were Not Linked to Business Goals

Leading organizations and NIST have stated that security measures need to be linked to an organization's overall business priorities to demonstrate their importance in accomplishing the organization's mission. However, nearly half of the measures developed by the 24 agencies were centered on four categories of security controls that are based on OMB's FISMA reporting requirements and not necessarily linked to the strategic goals of the agencies.¹⁴ Of the 5 agencies that provided information about their measures development process, only 1 agency explicitly linked its measures selection process to the agency's top IT priorities. Without explicitly linking information security program controls to agency-specific missions and business functions, an agency cannot ensure that its information security program is effectively supporting the organization's mission.

¹⁴The four NIST security controls categories addressed by these measures include (1) certification, accreditation, and security assessments; (2) configuration management; (3) planning (including system security planning, rules of behavior, and privacy impact assessments); and (4) system and information integrity.

Measures in Annual FISMA Reports Have Not Captured the Effectiveness of Federal Information Security Programs

While OMB has established a uniform set of 24 measures of information security programs that all federal agencies report on annually, OMB's practices for collecting and reporting these measures do not fully reflect key practices identified by leading organizations. Specifically, OMB collects few (3 of the 24) measures of programs' effectiveness, and the measures it collects do not include all key attributes. Further, OMB's annual report to Congress on information security also does not reflect key practices for communicating the effectiveness of an information security program. As a result, OMB is limited in its ability to report on the effectiveness of agency information security programs.

OMB's Ability to Assess Effectiveness of Federal Information Security Programs Has Been Limited by Reliance on Inadequate Performance Measures

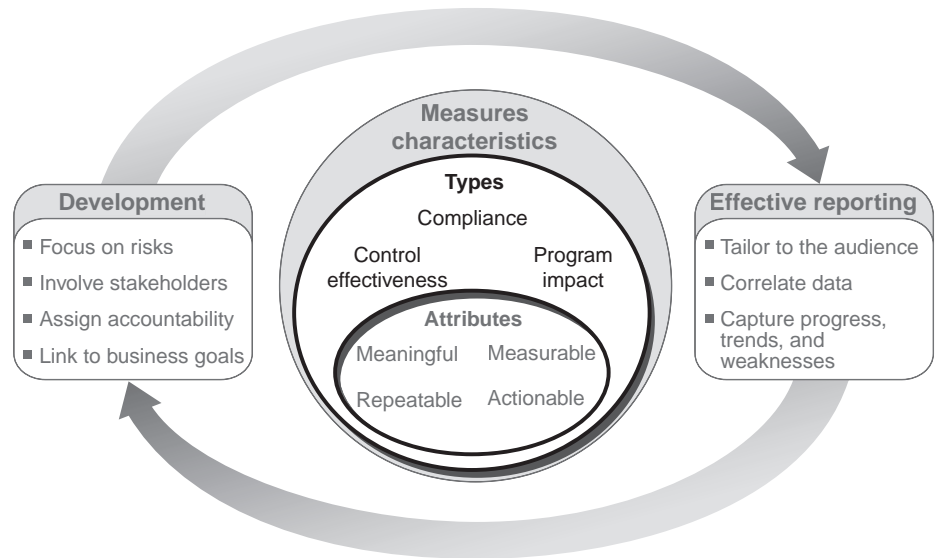
FISMA requires that the Director of OMB oversee the implementation of information security at federal agencies. To oversee agency compliance with FISMA, OMB relies in part on data provided annually by agencies and the Inspectors General and compares the reported data with security and privacy performance benchmarks that it has developed.¹⁵ Since 2003, OMB has required agencies to report on their implementation of information security control activities.

Required Measures Do Not Gauge the Effectiveness of Control Activities

OMB's 2008 FISMA reporting instructions specify primarily measures of compliance rather than measures of control effectiveness or program impact, as identified by leading organizations and NIST (see fig. 5). Specifically, the instructions include 18 compliance measures, 3 control effectiveness measures, and 3 program impact measures.

¹⁵OMB also takes some information from data submitted by agencies during the budget process, and other information comes from annual reports.

Figure 5: Measurement Types



Source: GAO.

Examples of the compliance measures OMB specified include

- the number and percentage of systems for which security controls have been tested,
- the number of agencies that have an agencywide security configuration policy, and
- the number and percentage of federal employees and contractors that have received security awareness training.

These measures are useful in that they help to determine the extent to which security controls that adhere to policies, standards, and other requirements are in place across federal agencies.

However, OMB's measures do not address the effectiveness of several key areas of information security controls, including, for example, agencies' security control testing and evaluation processes. Agencies are required to test and evaluate the effectiveness of controls over their systems at least once a year but are only required to report the number and percentage of systems undergoing such tests. 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.¹⁶ As a result, the measures collected by OMB cannot be used to determine the efficiency and effectiveness of agencies' security controls.

As another example, OMB did not request effectiveness measures for agencies' patch management activities.¹⁷ For patch management, OMB requested only that Inspectors General comment on whether they considered patching when assessing their agency's certification and accreditation rating. OMB did not collect direct measures of agency patch management processes. For example, there was no measure of whether patches were up to date, thoroughly tested before being applied in a production environment, or regularly monitored once deployed—all key elements of an effective patch management process.¹⁸ Our prior reports have identified weaknesses in agencies' patch management processes that leave information systems exposed to vulnerabilities associated with flaws in software code that could be exploited by malicious individuals to read, modify, or delete sensitive information or disrupt operations.¹⁹

We have testified that OMB's information security performance measures do not measure how effectively agencies are performing information security control activities and offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices.²⁰ We have recommended that OMB develop additional measures of the effectiveness of control activities.²¹ Until OMB develops such measures, it will not be able to adequately determine how well threats to

¹⁶OMB 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.

¹⁷Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. A component of configuration management, it includes acquiring, testing, applying, and monitoring adjustments, or "patches," to a computer system's software.

¹⁸See, for example, GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, [GAO-04-706](#) (Washington, D.C.: June 2, 2004).

¹⁹[GAO-07-837](#).

²⁰GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, [GAO-08-571T](#) (Washington, D.C.: Mar. 12, 2008).

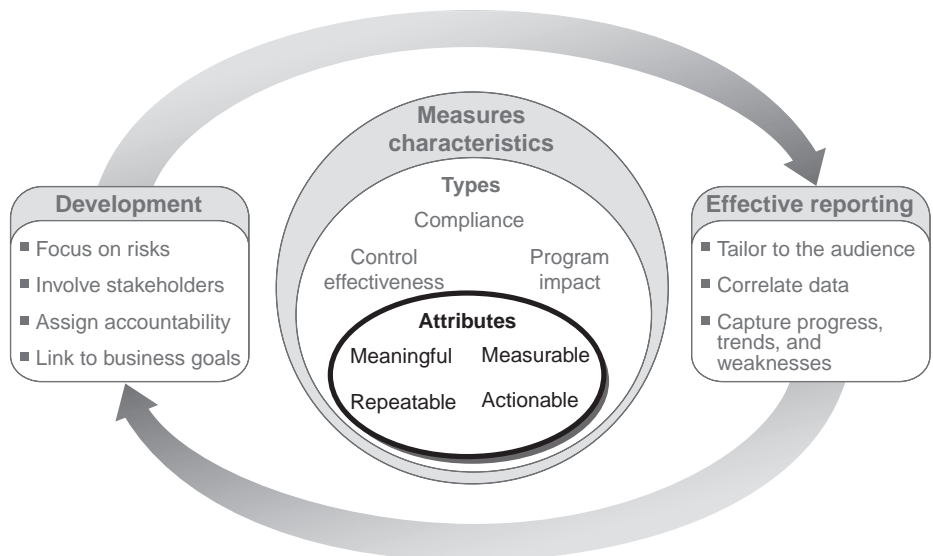
²¹[GAO-07-837](#).

the confidentiality, integrity, and reliability of federal information systems have been addressed, and it will continue to be limited in its ability to report on the effectiveness of federal information security efforts.

Not All Required Measures Include Key Attributes

While measures used by OMB to gauge agencies' information security programs in fiscal year 2008 usually included attributes identified by leading organizations, they did not always do so. Specifically, measurability, meaningfulness, and repeatability were not always included (see fig. 6).

Figure 6: Attributes of Measures



Source: GAO.

Not All Measures Are Based on Readily Measurable Values

As previously discussed, leading organizations stated that they aim to establish measures that can be expressed in discrete values, such as quantitative data (e.g., numbers, percentages), to ensure that the results are useful in decision making. Quantitative results can be used to facilitate comparisons for decision making and track actual versus expected performance. Moreover, quantitative measurements can be used as an objective foundation for developing higher-level summary measures that are more qualitative in nature.

For several measures in its 2008 FISMA guidance, OMB requested descriptive rather than quantitative information from federal agencies. For example, OMB asked agencies to describe

- their security control testing and continuous monitoring processes;
- tools, techniques, and technologies used for incident detection, handling, and response; and
- policies and procedures for using emerging technologies and countering emerging threats.

While descriptive information such as this offers useful insights into how agencies have developed their information security programs, it does not provide a measure of information security program effectiveness. For example, OMB reports to Congress on the extent to which policies and procedures for using emerging technologies and countering emerging threats exist at federal agencies, but it does not have a measure for the implementation and effectiveness of these policies and procedures. Measures could be developed to gauge how well agencies test their security controls or to evaluate their effectiveness. For example, OMB could develop measures that show effectiveness in monitoring emerging threats. As implemented by a financial institution, these could include the *percentage increase in incidents for [service provider or other third party] assets (e.g., systems, devices) connected to the network* or the *number and severity of audit issues related to [service provider or other third party] assets (e.g., systems, devices) connected to the network*, which can demonstrate the potential for security weaknesses at partner organizations to affect a parent organization's network. Supporting qualitative measures with observable conditions enables an organization to acquire a more robust view of effectiveness, as we have previously reported.²² In addition, a measure should be collected only if it is useful in the decision-making process.

Not All Measures Have Targets

Leading organizations stated that a factor in ensuring that measures are meaningful is that they have targets or thresholds to track progress over time. Organizations can enhance the usefulness of these measures by

²²GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, [GAO-03-143](#) (Washington, D.C.: Nov. 22, 2002).

tracking performance and subsequently directing resources to underperforming areas.

OMB has set implementation thresholds for several compliance measures in its FISMA guidance. These thresholds are generally associated with completeness or existence (e.g., “100 percent” or “Yes/No”). For example, the threshold for one measure is *percentage of agency and contractor systems certified and accredited is 100% as of this reporting period*.

However, not all of OMB’s performance measures have such targets. For example, agencies are required to report quarterly the number of plans of actions and milestones that are 90 to 120 days overdue. While this measure is intended to address the timeliness with which plans of actions and milestones are being executed, OMB has not established thresholds to indicate the acceptable number of overdue plans of actions and milestones within these time frames. As we have previously reported, performance measures should include such targets to facilitate assessments of whether overall goals and objectives have been achieved.²³

Certain OMB Measures Lack Repeatability and Consistency

Leading organizations developed measures that were repeatable and produced consistent results by ensuring that the measures were defensible and auditable, used readily obtainable data, and could be easily reproduced. Repeatable measures are the result of a measurement process that is applied consistently over time to ensure that measurements are comparable with each other. Use of such measures helps to reduce the likelihood of inaccuracies in or differing interpretations of the measures’ results.

In its FISMA reporting instructions, OMB specified a variety of agency information security measures, many of which appear to meet the criteria of being repeatable and producing consistent results. For example, OMB asks agencies to report on the number and percentage of systems certified and accredited as well as the number of agency and contractor systems by risk level.

However, a major component of the annual FISMA reports specified by OMB—evaluations by agency Inspectors General of agency information

²³ [GAO-03-143](#).

security activities—including several measures of key control activities that may not be repeatable or produce consistent results across agencies. For example, OMB's measure of agencies' certification and accreditation processes could lead to varying interpretations by Inspectors General. OMB directed Inspectors General to evaluate the quality of their agencies' certification and accreditation processes using the terms "excellent," "good," "satisfactory," "poor," or "failing." However, OMB did not specify what was to be measured and reflected in these assessments. Thus, the assessments were subject to differing interpretations by the Inspectors General, who may have varied in their understanding of what needs to be measured to conduct such an assessment. As a result, OMB's performance measure is unable to clearly reflect the Inspector General community's results.

We have also previously reported that several of the measures in OMB's FISMA guidance were unclear, including measures of the certification and accreditation process, which generated confusion.²⁴ We stated that without additional clarity, the measures would continue to be subject to differing interpretations, which may have reduced the overall reliability of the results. We recommended that OMB review its guidance to ensure clarity of instructions, and, in response, OMB stated that its staff worked with agencies and the Inspectors General when developing the guidance to ensure that agencies adequately understood the reporting instructions.

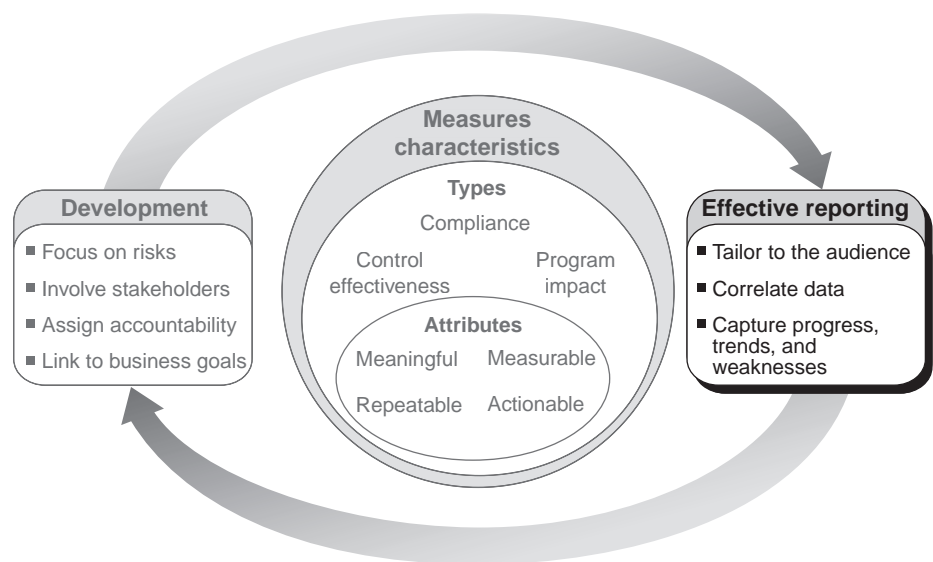
When measures lack key elements, the information that they derive becomes less useful and credible for management or oversight purposes. Until OMB ensures that all of its measures are based on measurable values, have defined targets, are clearly represented, and can be applied repeatedly and consistently, it will be limited in its ability to assess the effectiveness of federal agencies' information security programs.

²⁴See, for example, [GAO-05-552](#).

OMB's Use of Performance Measures in Its Annual Report to Congress Does Not Adequately Assess Federal Information Security Strengths and Weaknesses

As required by FISMA, OMB annually reports to Congress on the state of agencies' information security programs. The report is intended to provide an assessment of governmentwide information security strengths and weaknesses and outline a plan of action to improve performance. Effective use of measures in such a report would highlight progress and areas of improvement, and potentially drive behavior to better achieve program objectives. Leading organizations and security experts stated that communications regarding the results of information security measures should (1) be tailored to the audience; (2) correlate data; and (3) capture progress, trends, and weaknesses (see fig. 7).

Figure 7: Effective Reporting of Measures



Source: GAO.

However, OMB's report to Congress does not fully employ these practices and thus provides information of limited use about the effectiveness of agency information security programs.

OMB Did Not Tailor the Reporting of Its Measures to Congress

Leading organizations and experts state that tailoring the reporting of information security measures allows each audience to appropriately make strategic security decisions, formulate action plans, and identify areas where additional attention needs to be focused. OMB's report to

Congress includes information on how federal agencies are progressing in nine key security performance measures.²⁵ However, the report does not include sufficient information to support congressional decisions about the effectiveness of agency information security activities. For example, OMB's report merely summarizes the results of annual agency and Inspectors General reports in nine information security areas. In a section detailing action plans to improve performance, OMB simply states that it will be reviewing the security measures provided by agencies in their quarterly and annual reports for FISMA compliance. It further notes that the increased reported compliance by the agencies indicates that it could be time to modify the measures, but provides no further information about what modifications might be made. OMB also lists a goal for measures to move beyond periodic compliance reporting to more continuous monitoring of security but again does not discuss how this is to be achieved.

OMB Correlated Data to a Limited Extent to Provide Deeper Interpretation of Results

Leading organizations and experts stated that when reporting measures to executives and other decision makers, it is paramount to correlate the data from multiple individual measures to present more meaningful information. OMB did this to a limited extent in its 2008 report. For example, OMB summarized measures on agency systems inventories grouped by their respective risk levels with measures identifying the percentage of those systems that have (1) been certified and accredited, (2) tested contingency plans, and (3) tested security controls. The resulting information provided additional insight into whether agencies were appropriately prioritizing and focusing control activities on high-risk systems. However, OMB did not provide other correlations relative to the other measures it collects from the agencies. As a result, its ability to illustrate the effectiveness of agency information security programs was limited.

²⁵OMB's 2008 report to Congress presented information on progress in meeting key security performance measures in the areas of certification and accreditation, testing of contingency plans and security controls, inventory of systems, quality of certification and accreditation process, identifying risk impact level, employee training in systems security, oversight of contractor systems, agencywide plan of action and milestones, and configuration management.

Report Captured Some Progress but Did Not Discuss Trends and Weaknesses

As previously discussed, leading organizations structured their communications about information security measures to include data on progress, trends, and weaknesses or deficiencies in information security controls. Including trend data helps illustrate improving or declining performance by comparing data points over time. OMB's 2008 report provided only limited information on the progress of selected controls. In its report, OMB provided data on progress for four of the nine areas contained in its report but did not explain why it did not include progress data for the other areas and also did not report on trends and weaknesses. For example, OMB provided data on the progress of agencies whose contingency plans and security controls were tested from 2002 through 2008. OMB provided no further details to support assessments by Congress of the effectiveness of agency programs since the enactment of FISMA in 2002. As a result, Congress was not provided sufficient information to fully determine whether the performance of key security controls at federal agencies was improving or declining.

Effective reporting of information security program measures is essential to informing decision makers of those programs' performance. Until OMB begins to collect effectiveness measures and report their results through key practices such as tailoring measures to the audience; correlating data to derive greater meaning; and capturing progress, trends, and deficiencies of security controls, the utility of its reports to Congress on the effectiveness of federal information security programs will be limited.

Conclusions

Federal agencies have developed information security performance measures that in many cases adhere to key practices endorsed by leading organizations and experts, which correlate with NIST guidance that OMB requires agencies to follow. However, agency measures do not always adhere to these key practices. Much of the emphasis at agencies continues to be on collecting and reporting the most basic of performance measures—measures of compliance. These measures are of only limited value in understanding the security posture of federal agencies. The primary reason that agencies emphasize basic compliance measures is that OMB has focused on these measures, setting specific requirements for reporting on them. Until OMB revises its reporting guidance to require a more balanced range of measures and adherence to key practices in developing those measures, agencies are likely to continue to

predominantly rely on measures that are of only limited value in assessing the effectiveness of their information security programs.

OMB has compiled annual reports on agency information security programs that focus on the extent to which security controls that adhere to policies, standards, and other requirements are in place. However, OMB has not fully adopted key practices in collecting measures data from agencies and reporting the results to Congress. The specific data elements that OMB required agencies to report have been largely inadequate to measure the effectiveness of federal information security programs, and OMB has not sufficiently used key practices, such as correlating the data and discussing trends and weaknesses, that would have provided a more complete and valuable assessment. Until OMB revises its reporting requirements and enhances its reporting of information security measures, Congress will remain constrained in its ability to assess the status of federal information security programs and the progress that has been made in addressing information security risks in the federal government.

Recommendations for Executive Action

To assist federal agencies in developing and using measures that better address the effectiveness of their information security programs, we are recommending that the Director of the OMB take the following three actions:

- Issue revised information security guidance to agency chief information officers (CIO) reinforcing the existing requirement that agencies follow NIST guidance (which correlates with key practices) in developing measures and clarifying the need to develop and use a balanced set of measures that includes compliance, control effectiveness, and program impact measures.
- Direct agency CIOs to ensure that all of their measures exhibit the four key attributes of a measure (i.e., that it be measurable, meaningful, repeatable and consistent, and actionable).
- Direct agency CIOs to employ key practices identified by leading organizations in developing their measures (i.e., focusing on risk, involving key stakeholders in development, assigning accountability, and linking measures to business goals).

To improve OMB's process for collecting measures and reporting to Congress on the status of information security programs, we are recommending that the Director of OMB take the following two actions:

-
- Revise annual reporting guidance to agencies to require (1) reporting on a balanced set of measures, including measures that focus on the effectiveness of control activities and program impact, and (2) inclusion of all key attributes in the development of measures.
 - Revise the annual report to Congress to provide better status information, including information on the effectiveness of agency information security programs, the extent to which major risks are being addressed, and progress that has been made in improving the security posture of the federal government.

Agency Comments

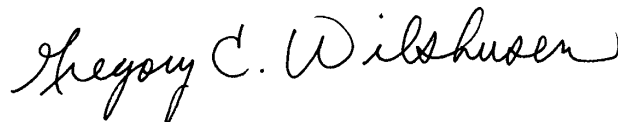
In providing oral comments on a draft of this report, representatives of OMB's Office of E-Government and Information Technology stated that they generally agreed with the contents and recommendations of the report.

We also provided a draft of this report to 24 major federal agencies. Of the 24 agencies, 6 agreed with the contents of our report, 17 responded that they had no comments, and 1 agency did not respond.

As we agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to interested congressional committees and to the Director of OMB. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) describe key types and attributes of performance measures, (2) identify the practices of leading organizations for using measures to guide and monitor their information security control activities, (3) identify what measures federal agencies use to guide and monitor their information security control activities and how they are developed, and (4) identify the effectiveness of the measures-reporting practices that the federal government uses to inform Congress about the effectiveness of information security programs.

To describe the key types and attributes, we met with organizations we identified as part of our second objective. We obtained information through interviews with senior officials of leading organizations and security experts, and through our review of National Institute of Standards and Technology (NIST) guidance. We then analyzed the information we obtained from all sources to identify key attributes and characteristics.

To identify the practices of leading organizations, we first identified these organizations by reviewing information security-related Web sites, professional literature, and research information and solicited suggestions from experts in professional organizations, the National Association of State Chief Information Officers, a nationally known public accounting firm, and a federal agency, because they were in a position to evaluate and compare information security programs at numerous organizations. In addition, we attempted to select organizations from a variety of business sectors to gain a broad perspective on the information security practices being employed. We selected organizations that (1) process or possess sensitive information that needs to be protected;¹ (2) manage operations of a regional, national, or international scope; (3) have multiple components with varying operational functions and/or lines of business; and (4) operate computing environments that are comparable to those of federal agencies, specifically the 24 major federal agencies. We identified 35 organizations that met our criteria, 14 of which agreed to participate in our review. Each organization we contacted had an enterprisewide information security program. All were prominent, nationally known organizations. They included a nonprofit computer security organization; two financial services corporations; a manufacturer; three universities; a global technology, media, and financial services company; two state agencies; a nonbank financial institution; a security technology company;

¹Sensitive information is any information that an agency has determined requires some degree of heightened protection from unauthorized access, use, disclosure, disruption, modification, or destruction because of the nature of the information.

a global defense technologies developer and services provider; and a global communications company.

To identify key practices, we obtained information, primarily through interviews with senior officials at leading organizations and document analysis conducted during and after visits to the organizations we studied. We supplemented the information gathered from leading organizations with information obtained from four information security experts. These experts were selected based on recommendations from a federal agency and organizations we met with as well as our independent research.

To determine measures used and developed by federal agencies, we collected and analyzed agency-specific measures, policies, plans, and practices related to information security measures through a data request to 24 major federal agencies. All 24 agencies responded to our data requests. We met with officials from these agencies to obtain additional information and clarification when necessary. We then content analyzed the results from the data requests to identify the types of measures and measures development practices used by agencies. We took steps in the data analysis to eliminate errors. For example, for each agency, two analysts compared their independent results of the analyses performed. If the results did not match, the analysts discussed the anomalies and reached a final consensus.

To determine the effectiveness of the federal government's practices for reporting performance measures, we reviewed prior GAO reports and relevant laws and guidance such as the Federal Information Security Management Act of 2002 (FISMA) to identify mandatory and optional practices for reporting information security program information (including performance measurement information) to the Office of Management and Budget (OMB) and Congress. Additionally, we researched official publications issued by OMB and NIST to identify policies, standards, and guidance on reporting practices. We then compared these practices with those identified by leading organizations to determine their effectiveness.

We conducted this performance audit from July 2008 through September 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: References on Information Security Measures

Table 1 lists a selection of publications, Web sites, and other resources consulted during the course of our review.

Table 1: References on Information Security Performance Measures

Resource	Description
The Center for Internet Security, <i>The CIS Security Metrics</i> (May 11, 2009).	Provides 20 potentially actionable information security performance measures within the context of seven business functions—incident management, vulnerability management, patch management, application security, configuration management, financial metrics, and future functions.
Consensus Group of Government and Industry Security Experts, <i>Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines</i> , version 2.0 (Bethesda, Maryland: May 9, 2009).	Proposes a list of 20 critical security controls to combat existing and future high-priority attacks.
Information Assurance Technology Analysis Center, <i>Measuring Cyber Security and Information Assurance: State-of-the-Art Report</i> (Herndon, Virginia: May 8, 2009).	Presents the current state of cyber security and information assurance approaches for developing measures.
Securitymetrics.org, www.securitymetrics.org (accessed May 8, 2009).	Offers resources on the topic of security metrics for security practitioners, including information on a security metrics conference and links to other relevant guidance.
Martin, Robert A., <i>Making Security Measurable and Manageable</i> (Bedford, Massachusetts, MITRE Corp., 2008), http://makingsecuritymeasurable.mitre.org/about/Making_Security_Measurable_and_Manageable.pdf (accessed May 6, 2009).	Offers advice for employing automation tools and practices in order to measure and manage cyber security assets.
Committee on Metrics for Global Change Research Climate Research Committee Board on Atmospheric Sciences and Climate Division on Earth and Life Studies, National Research Council of the National Academies, <i>Thinking Strategically: The Appropriate Use of Metrics for the Climate Change Science Program</i> (Washington D.C.: National Academies Press, 2005), http://www.nap.edu/catalog/11292.html (downloaded August 24, 2009).	Discusses quantitative metrics and performance measures for documenting progress and evaluating future performance for selected areas of global change and climate change research.
Allen, Julia, and Clint Kreitner, <i>Getting to a Useful Set of Security Metrics</i> , http://www.cert.org/podcast/show/20080902kreitner.html (September 2, 2008, transcript accessed January 16, 2009).	Discusses challenges and opportunities in creating a common set of widely accepted security metrics that business leaders and security professionals can use to make better informed decisions.
Kark, Khalid, <i>Case Study: Verizon Business Builds An Asset-Based Security Metrics Program</i> (Forrester Research, Inc., July 22, 2008), www.forrester.com (downloaded October 7, 2008).	Identifies practices of one organization's business metrics program and its use of asset-based testing and measurement.
Kark, Khalid, <i>Best Practices: Security Metrics</i> (Forrester Research, Inc., July 22, 2008), www.forrester.com (downloaded October 7, 2008).	Identifies challenges of using security metrics and offers guiding principles based on interviews with 20 chief information security officers.

Appendix II: References on Information Security Measures

Resource	Description
Bartol, Nadya, <i>Practical Measurement Framework for Software Assurance and Information Security</i> , Version 1.0, draft (Booz Allen Hamilton: October 2008).	Provides an approach for measuring the effectiveness of achieving software assurance goals and objectives at an organizational, program, or project level using quantitative and qualitative measurement methodologies.
NIST, Special Publication 800-55 Revision 1, <i>Performance Measurement Guide for Information Security</i> (Gaithersburg, Maryland: July 1, 2008).	Provides guidance to assist federal agencies in the development, selection, and implementation of information security measures at the system and program levels. The publication also provides a framework for quantifying the implementation and effectiveness of policies and practices with respect to security control objectives and techniques, using the NIST SP 800-53 ^a framework of security controls as the basis for developing measures.
Allen, Julia, and Sam Merrell, <i>Initiating a Security Metrics Program: Key Points to Consider</i> , http://www.cert.org/podcast/show/20080318merrell.html (March 18, 2008, transcript accessed January 16, 2009).	Identifies challenges and factors to consider in developing a security metrics program.
Allen, Julia, and Betsy Nichols, <i>Building a Security Metrics Program</i> , http://www.cert.org/podcast/show/20080205nichols.html (February 5, 2008, transcript accessed October 8, 2008).	Discusses challenges in selecting, gathering, and collecting security metrics and approaches to initiating a security metrics program.
Wheatman, Jeffrey, <i>Toolkit Best Practices: Selecting Security Metrics</i> (Gartner, Inc., September 26, 2007), www.gartner.com (downloaded October 7, 2008).	Discusses promising practices for developing effective security metrics.
Wheatman, Jeffrey, <i>The Do's and Don'ts of Information Security Metrics</i> (Gartner, Inc., September 26, 2007), www.gartner.com (downloaded October 28, 2008).	Discusses critical factors for an effective security metrics program as well as examples of generally good or generally poor metrics associated with each critical factor.
Kark, Khalid, and Paul Stamp, <i>Defining an Effective Security Metrics Program</i> (Forrester Research, Inc., May 17, 2007), www.forrester.com (downloaded May 7, 2009).	Discusses the need to identify, prioritize, monitor, and measure security based on business goals and objectives and provides guidance on communicating results for executive decision making.
Jaquith, Andrew, <i>Security Metrics: Replacing Fear, Uncertainty, and Doubt</i> (Upper Saddle River, New Jersey: Addison-Wesley, 2007).	Discusses lessons learned and challenges facing practitioners attempting to measure information security performance. It includes, among other things, examples of metrics that can be tailored to measure the effectiveness of both technical and program performance and strategies for ensuring effective communication of metrics results.
Hermann, Debra S., <i>Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI</i> (Boca Raton, Florida: Auerbach Publications Taylor and Francis Group, 2007).	Provides advice on how to develop and apply security performance measures to the physical, personnel, information technology, and operational security domains. According to the author, it contains an index of approximately 900 metrics that organizations can tailor to meet their performance measurement requirements.
Payne, Shirley C., <i>A Guide to Security Metrics</i> , Version 1.2e (Bethesda, Maryland: The SANS Institute, June 19, 2006).	Offers information regarding basic principles of information security metrics and includes a proposed definition of security metrics and process for developing a security metrics program.
Campbell, George K., <i>Measures and Metrics in Corporate Security</i> (The Security Executive Council, 2006).	Provides advice on building a security metrics program that aligns with business goals, discusses approaches to addressing possible organizational concerns, and provides examples of security-related metrics and measures that communicate security implications to a variety of groups.

Appendix II: References on Information Security Measures

Resource	Description
Government Reform Committee, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, United States House of Representatives, <i>Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams</i> , November 17, 2004 (Revised January 10, 2005).	Provides approximately 100 potentially actionable information security performance metrics within the context of three different levels of organizational responsibility for an information security program—Governance, Management, and Technical—and program elements (practices) to be considered at each of the levels.
NIST, ITL Bulletin, <i>IT Security Metrics</i> (Gaithersburg, Maryland: August, 2003).	Summarizes information from other NIST guidance on information security performance measurement, including a metrics development process.
Lowans, Paul W., <i>Implementing a Network Security Metrics Program</i> , Version 2.0 (Bethesda, Maryland: the SANS Institute, 2000-2002).	Suggests linkages between software metrics and information security metrics programs. The work includes examples of security metrics to be implemented and common pitfalls for security metrics programs to avoid, among other things.
Information Assurance Technology Analysis Center, <i>IA Metrics: Critical Review & Technology Assessment (CR/TA) Report</i> (June 1, 2000).	Discusses, within the context of information assurance, approaches to developing metrics, implementing metrics program elements, and analyzing metrics.

Source: GAO.

^aNational Institute of Standards and Technology, *Special Publication 800-53 Revision 2: Recommended Security Controls for Federal Information Systems* (Gaithersburg, Md.: December 2007).

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgements

In addition to the individual named above, John de Ferrari and Anjalique Lawrence (Assistant Directors), Ashley Brooks, Season Dietrich, Neil Doherty, Ronalynn Espedido, Min Hyun, Joshua Leiling, Lee McCracken, and David Plocher made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

