NIST Special Publication 800-55

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Security Metrics Guide for Information Technology Systems

Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

July 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON: 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office

Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250

Mail: Stop SSOP, Washington, DC 20402-0001

Authority

This document has been developed by NIST in furtherance of its statutory responsibilities under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996 (specifically 15 United States Code (U.S.C.) 278 g-3 (a)(5)). This is not a guideline within the meaning of 15 U.S.C 278 g-3 (a)(3).

These guidelines are for use by Federal organizations which process sensitive information. They are consistent with the requirements of OMB Circular A-130, Appendix III.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon federal agencies by the Secretary of Commerce under his statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

The authors wish to thank Elizabeth Lennon (NIST), Richard Kissel (NIST), Will Robinson (Booz Allen Hamilton), and Matt Dombrowski (Booz Allen Hamilton) who reviewed drafts of this document and contributed to its development. We would like to thank Ellen Roth and Gail Brown (Booz Allen Hamilton) for the development and delivery of the metrics workshop. We would also like to acknowledge the contributions of the NIST/CIO Council Metrics Working Group.

TABLE OF CONTENTS

FIGURES AND TABLES

EXECUTIVE SUMMARY

The requirement to measure IT security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite IT performance measurement in general, and IT security performance measurement in particular, as a requirement. These laws include the Clinger-Cohen Act, Government Performance and Results Act (GPRA), Government Paperwork Elimination Act (GPEA), and Federal Information Security Management Act (FISMA).

This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. IT security metrics must be based on IT security performance goals and objectives. IT security performance goals state the desired results of a system security program implementation. IT security performance objectives enable accomplishment of goals by identifying practices defined by security policies and procedures that direct consistent implementation of security controls across the organization. IT security metrics monitor the accomplishment of the goals and objectives by quantifying the level of implementation of the security controls and the effectiveness and efficiency of the controls, analyzing the adequacy of security activities and identifying possible improvement actions. This document provides examples of metrics based on the critical elements and security controls and techniques contained in NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems.* During metrics development, goals and objectives from federal, internal, and external guidance, legislation, and regulations are identified and prioritized to ensure that the measurable aspects of security performance correspond to operational priorities of the organization.

The following matters must be considered during development and implementation of IT security metrics program:

- Metrics must yield quantifiable information (percentages, averages, and numbers)
- Data supporting metrics needs to be readily obtainable
- Only repeatable processes should be considered for measurement
- Metrics must be useful for tracking performance and directing resources.

Metrics development process, described in this document, ensures that the metrics are developed with the purpose of identifying causes of poor performance and therefore point to appropriate corrective actions.

Organizations can develop and collect metrics of three types:

- Implementation metrics to measure implementation of security policy
- Effectiveness/efficiency metrics to measure results of security services delivery
- Impact metrics to measure business or mission impact of security events.

The types of metrics that can realistically be obtained and that can also be useful for performance improvement depend on the maturity of the agency's security program and the system's security control implementation. Although different types of metrics can be used simultaneously, the primary focus of IT security metrics shifts as the implementation of security controls matures.

1. INTRODUCTION

The requirement to measure information technology (IT) security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite IT performance measurement in general, and IT security performance measurement in particular, as a requirement. These laws include the Clinger-Cohen Act, Government Performance and Results Act (GPRA), Government Paperwork Elimination Act (GPEA), and Federal Information Security Management Act (FISMA).

This document is intended to be a guide for the specific development, selection, and implementation of IT system-level metrics to be used to measure the performance of information security controls and techniques.[1] IT security metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metrics development and implementation processes and how metrics can be used to adequately justify security control investments. The results of an effective IT security metrics program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports. Successful implementation of such a program assists agencies in meeting the annual requirements of the Office of Management and Budget (OMB) to report the status of agency IT security programs.

1.1 History

The approach for measuring IT security controls and techniques has been under development for numerous years. This document builds on these past efforts and presents an approach that aligns with the security control objectives and techniques contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems.*

Security control objectives and techniques for systems and programs are reviewed and reported annually to OMB in accordance with the Electronic Government Act of 2002, which includes the Federal Information Security Management Act commonly referred to as FISMA. The act requires departments and agencies to demonstrate that they are meeting applicable security requirements and to document the actual level of performance based on the results of annual program reviews.

On May 21, 2002, the NIST Federal Computer Security Program Managers' Forum sponsored two IT security metrics workshops designed to help federal personnel with OMB fiscal year (FY)

[1] The word "system" is used as an aggregate term to signify Major Applications (MA) and General Support Systems (GSS) as defined by the Office of Management and Budget (OMB) Circular A-130, Appendix III.

2002 Government Information Security Reform Act (GISRA) draft reporting guidance. GISRA, which is a part of the Public Law 106 398, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, was replaced by FISMA in December 2002. Approximately 75 federal government employees attended these workshops, where they learned to develop IT security metrics that map to NIST SP 800-26 critical elements. This document, NIST SP 800-55, captures the proceedings of the workshops, including the original metrics developed by the breakout groups, expands on the topics presented in the workshops, and contains example metrics and implementation guidance for using the metrics.

1.2 Overview of Metrics Program

A security metrics program within an organization should include four interdependent components (see Figure 1-1).

Figure 1-1. Security Metrics Program Structure

The foundation of strong upper-level management support is critical, not only for the success of the security program, but also for the implementation of a security metrics program. This support establishes a focus on security within the highest levels of the organization. Without a solid foundation (i.e., proactive support of those persons in positions that control IT resources), the effectiveness of the security metrics program can fail when pressured by politics and budget limitations.

The second component of an effective security metrics program is practical security policies and procedures backed by the authority necessary to enforce compliance. Practical security policies

and procedures are defined as those that are attainable and provide meaningful security through appropriate controls. Metrics are not easily obtainable if there are no procedures in place.

The third component is developing and establishing quantifiable performance metrics that are designed to capture and provide meaningful performance data. To provide meaningful data, quantifiable security metrics must be based on IT security performance goals and objectives, and be easily obtainable and feasible to measure. They must also be repeatable, provide relevant performance trends over time, and be useful for tracking performance and directing resources.

Finally, the security metrics program itself must emphasize consistent periodic analysis of the metrics data. The results of this analysis are used to apply lessons learned, improve the effectiveness of existing security controls, and plan future controls to meet new security requirements as they occur. Accurate data collection must be a priority with stakeholders and users if the collected data is to be meaningful to the management and improvement of the overall security program.

The success of an information security program implementation should be judged by the degree to which meaningful results are produced. A comprehensive security metrics analysis program should provide substantive justification for decisions that directly affect the security posture of an organization. These decisions include budget and personnel requests and allocation of available resources. A security metrics program should provide a precise basis for preparation of required security performance-related reports.

1.3 Relationship to Other NIST Documents

This document is a continuation in a series of NIST special publications intended to assist IT management and security personnel in the establishment, implementation, and maintenance of an IT security program. NIST SP 800-26 identifies five management control topic areas, nine operational control topic areas, and three technical control topic areas that affect the security posture of an organization. This document provides a recommended methodology for quantifying the critical elements in NIST SP 800-26 and for validating the implementation and effectiveness of the system security control objectives and techniques.

1.4 Audience

This document provides guidance for IT managers and security professionals at all levels, inside and outside the government.

1.5 Document Organization

The remaining sections of this guide discuss the following:

- Section 2 – Roles and Responsibilities, describes the roles and responsibilities of the agency staff that have a direct interest in the success of the IT security program, and in the establishment of a security metrics program.

- Section 3 – IT Security Metrics Background**,** provides guidance on the background and definition of Security Metrics, the benefits of implementation, various types of security metrics, and the factors which directly affect the success of a security metrics program.

- Section 4 – Metrics Development, presents the approach and process used for the development of useful IT security metrics.

- Section 5 – Metrics Program Implementation, discusses those factors that can affect the technical implementation of a security metrics program.

This guide also contains three appendices. Appendix A – Computer Security Metrics Examples, provides practical examples of security metrics that can be used or modified to meet specific agency requirements. Appendix B provides a list of acronyms used in this document. Appendix C lists references.

2. ROLES AND RESPONSIBILITIES

This section outlines the key roles and responsibilities for developing and implementing IT security metrics.

2.1 Head of the Agency

The head of the agency is held accountable for the security posture of the organization's IT infrastructure. This position controls the resource budget and has ultimate management responsibility for resource allocation. The head of the agency has the following responsibilities related to IT security performance metrics:

- Demonstrates support for IT security metrics development and implementation, and communicates official support to the agency
- Ensures that the program has adequate financial and human resources for success
- Actively promotes IT security metrics as an essential facilitator of IT security performance improvement throughout the agency
- Approves policy to officially institute metrics and the development and implementation of metrics
- Motivates program managers and ensures that they develop and use metrics in support of the information security program.

2.2 Chief Information Officer

The Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act) requires agencies to appoint Chief Information Officers (CIOs) and to use business process reengineering and performance measures to ensure effective IT procurement and implementation.

The CIO has the following responsibilities related to IT security metrics:

- Demonstrates management's commitment to IT security metrics development and implementation through formal leadership.
- Formally communicates the importance of using IT security metrics to monitor the overall health of the IT security program and to comply with applicable regulations
- Ensures IT security metrics program development and implementation
- Allocates adequate financial and human resources to the program

- Communicates with program managers/system owners to facilitate metrics acceptance and build support for the program

- Empowers IT metrics collection

- Reviews IT security metrics regularly and uses IT security metrics data to support policy, resource allocation, budget decisions, and an understanding of the IT security program posture.

- Ensures that a process is in place to address issues discovered through metrics analysis and takes corrective actions, such as revising security procedures and providing additional security training to staff

- Issues policy, procedures, and guidance to officially develop, implement, and institute metrics.

2.3 Agency IT Security Program Manager[2]

This position is known by different names, such as Deputy CIO for Cyber Security, Deputy CIO for IT Security, or Information System Security Officer (ISSO). This is an official whose primary responsibility is IT security agency wide. The IT Security Program Manager has the following responsibilities related to IT security metrics:

- Leads IT security metrics program development and implementation

- Ensures a standard process is used throughout the agency for metrics development, creation, and analysis

- Leads development of any internal guidance or policy related to IT security metrics

- Obtains qualified government staff and/or contractor support for program development and implementation

- Obtains adequate financial resources to support program development and implementation

- Actively solicits input from and provides feedback to the program manager/system owner at every step of program development

- Ensures that metrics data is collected, analyzed, and reported to the CIO and agency program manager/system owner

[2] Under FISMA this position is titled Senior Agency Information Security Officer.

- Reviews IT security metrics regularly, and uses IT security metrics data as support for policy, resource allocation, budget decisions, and insight into the health of the IT security program

- Educates program managers/system owners about using results of IT security metrics for policy, resource allocation, and budget decisions

- Ensures adequate maintenance of the program, in which the metrics that have reached their performance target are phased out and new metrics are developed and used

- Ensures manageability of the program by limiting the number of collected metrics at a single point in time to between 10 and 20 metrics

- Ensures prioritization of metrics to address high-priority items and problem areas

- Ensures that the corrective actions, identified through measuring IT security performance, are implemented.

2.4 Program Manager/System Owner

System and information owners are responsible for ensuring that proper controls are in place to address confidentiality, integrity, and availability of the IT systems and the owners' data. The program manager/system owner has the following responsibilities related to IT security metrics:

- Participates in IT security metrics program development and implementation by providing feedback on the feasibility of data collection and identifies data sources and repositories

- Educates staff about the development, collection, and analysis of IT security metrics and how it will affect IT security policy, requirements, resource allocation, and budget decisions

- Ensures that metrics data is collected consistently and accurately and is provided to designated staff that are analyzing and reporting the data

- Directs full participation and cooperation of staff, when required

- Reviews IT security metrics data regularly and uses it for policy, resource allocation, and budget decisions

- Supports implementation of corrective actions, identified through measuring IT security performance.

2.5 System Security Officer

The term System Security Officer, used in this document, means an individual assigned responsibility for security of a specific program or system within an agency or a department. The System Security Officer has the following responsibilities related to IT security metrics:

- Manages day-to-day program development and implementation
- Collects data or provides metrics data to designated staff that are collecting, analyzing, and reporting the data
- Assists with implementation of corrective actions identified when measuring IT security performance.

3. IT SECURITY METRICS BACKGROUND

This section provides basic information on what metrics are and why IT security performance should be measured. Additionally, this section defines types of metrics that can be used to measure IT security controls, discusses the key aspects of making a metrics program successful, and identifies the uses of metrics for management, reporting, and decision making.

3.1 Definition

Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related 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.

IT security metrics can be obtained at different levels within an organization. Detailed metrics, collected at the system level, can be aggregated and rolled up to progressively higher levels, depending on the size and complexity of an organization. While a case can be made for using different terms for more detailed and aggregated items, such as "metrics" and "measures," this document uses these terms interchangeably.

IT security metrics must be based on IT security performance goals and objectives. IT security performance goals state the desired results of a system security program implementation, such as "All employees should receive adequate security awareness training." IT security performance objectives enable accomplishment of goals by identifying practices defined by security policies and procedures that direct consistent implementation of security controls across the organization. Examples of IT security performance objectives, corresponding to the example goal cited above are "All new employees receive new employee training," "Employee training includes a summary of the Rules of Behavior," and "Employee training includes a summary and a reference to the organization's security policies and procedures." IT security metrics monitor the accomplishment of the goals and objectives by quantifying implementation of the security controls and the effectiveness and efficiency of the controls, analyzing the adequacy of security activities, and identifying possible improvement actions. During metrics development, goals and objectives from federal, internal, and external guidance, legislation, and regulations are identified and prioritized to ensure that the measurable aspects of security performance correspond to operational priorities of the organization.

IT security metrics must yield quantifiable information for comparison purposes, apply formulas for analysis, and track changes using the same points of reference. Percentages or averages are most common, and absolute numbers are sometimes useful, depending on the activity that is being measured.

Data required for calculating metrics must be readily obtainable, and the process that is under consideration needs to be measurable. Only processes that can be consistent and repeatable should be considered for measurement. Although the processes may be repeatable and stable,

the measurable data may be difficult to obtain. Metrics must use easily obtainable data to ensure that the burden of measurement on the organization does not defeat the purpose of measurement by absorbing the resources that may be needed elsewhere.

To be useful for tracking performance and directing resources, metrics need to provide relevant performance trends over time and point to improvement actions that can be applied to problem areas. Management should use metrics to assess performance by reviewing metrics trends, identifying and prioritizing corrective actions, and directing the application of those corrective actions based on risk mitigation factors and available resources. The metrics development process, described in Section 4, ensures that the metrics are developed with the purpose of identifying causes of poor performance and therefore point to appropriate corrective actions.

3.2 Benefits of Using Metrics

A security metrics program provides a number of organizational and financial benefits. Organizations can improve accountability for security by deploying IT security metrics. The process of data collection and reporting will enable the management to pinpoint specific technical, operational, or management controls that are not being implemented or are implemented incorrectly. IT security metrics can be created to measure each aspect of the organization's security. For example, the results of risk assessments, penetration testing, security testing and evaluation, and other security-related activities can be quantified and used as data sources for metrics. Using the results of the metrics analysis, program managers and system owners can isolate problems, use collected data to justify investment requests, and then target investments specifically to the areas in need of improvement. By using metrics to target security investments, organizations can get the best value from available resources.

Departments and agencies can demonstrate compliance with applicable laws, rules, and regulations by implementing and maintaining an IT security metrics program as described in this document. IT security metrics will assist in satisfying the annual FISMA reporting requirement to state performance measures for past and current fiscal years. Additionally, IT security metrics can be used as input into the General Accounting Office (GAO) and Inspectors General (IG) audits. Implementation of an IT security metrics program will demonstrate agency commitment to proactive security. It will also greatly reduce time spent by agencies collecting the data, which is routinely requested by GAO and IG during audits and for subsequent status updates. The implementation of an IT security metrics program means that the requested data may have been tracked, collected, and analyzed as a part of a regular metrics program operation.

Fiscal constraints and market conditions compel government and industry to operate on reduced budgets. In such an environment, it is difficult to justify broad investments in the IT security infrastructure. Historically, arguments for investing in specific areas of IT security lack detail and specificity, and fail to adequately mitigate specific system risk. Use of IT security metrics will allow organizations to measure successes and failures of past and current security investments and should provide quantifiable data that will support allocation of resources for future investments. IT security metrics can also assist with determining effectiveness of implemented IT security processes, procedures, and controls by relating results of IT security

activities (e.g., incident data, revenue lost to cyber attacks) to the respective requirements and to IT security investments.

3.3 Metrics Types

The maturity of an organization's IT security program determines the type of metrics that can be gathered successfully as depicted in Figure 3-1.

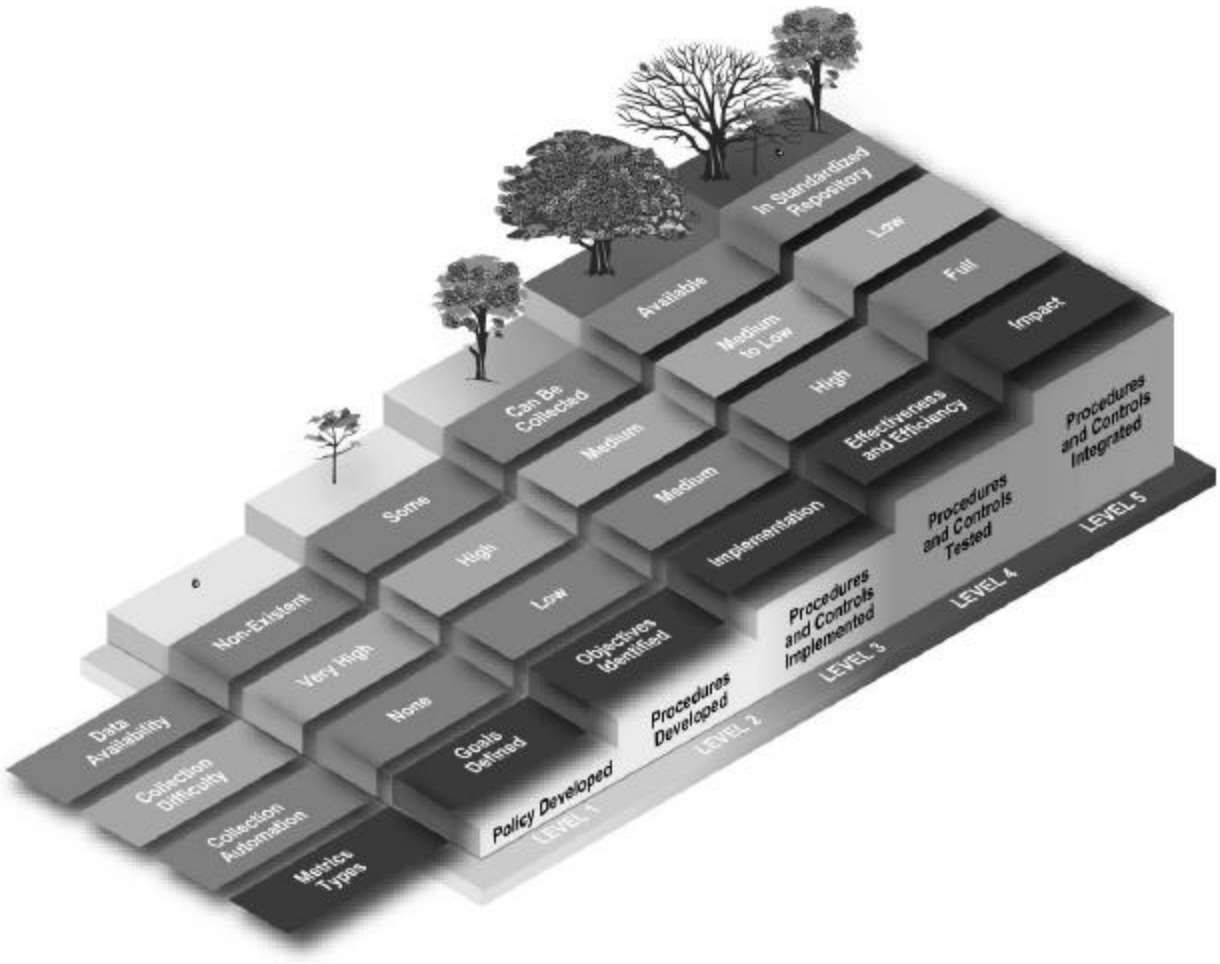

Figure 3-1. Security Program Maturity and Types of Measurement

A program's maturity is defined by the existence and institutionalization of processes and procedures. As a security program matures, its policies become more detailed and better documented, the processes that it uses become more standardized and institutionalized, and it produces data that can be used for performance measurement in greater quantity. According to NIST SP 800-26, the security program progresses from having policies (Level 1) to having detailed procedures (Level 2), implementing these procedures (Level 3), testing compliance with and effectiveness of the procedures (Level 4), and finally fully integrating policies and procedures into daily operations (Level 5). A mature program normally deploys multiple

tracking mechanisms to document and quantify various aspects of its performance. As more data becomes available, the difficulty of measurement decreases, and the ability to automate data collection increases. Data collection automation depends on the availability of data from automated sources versus the availability of data from people. Manual data collection involves developing questionnaires and conducting interviews and surveys with the organization's staff. More useful data becomes available from semi automated and automated data sources, such as self-assessment tools, certification and accreditation (C&A) databases, incident reporting and response databases, and other data sources as a security program matures. Metrics data collection is fully automated when all data is gathered by using automated data sources without human involvement or intervention.

The types of metrics (implementation, efficiency and effectiveness, and impact) that can realistically be obtained and that can also be useful for performance improvement depend on the maturity of the security control implementation. Although different types of metrics can be used simultaneously, the primary focus of IT security metrics shifts as the implementation of security controls matures. When security controls have been defined in procedures and are in the process of being implemented, the primary focus of metrics will be on the level of implementation of security controls. Examples of implementation metrics that are applied at this level of maturity are the percentage of systems with approved security plans and the percentage of systems with password policies configured as required. When a system progresses through Level 1 and Level 2, the results of these metrics will be less than 100 percent, indicating that the system has not yet reached Level 3. When the metrics implementation results reach and remain at 100 percent, it can be concluded that the system has fully implemented security controls and has reached Level 3.

As security controls are documented and implemented, the ability to reliably collect the outcome of their implementation improves. As an organization's IT security program evolves and performance data becomes more readily available, metrics will focus on program efficiency—timeliness of security service delivery and effectiveness—operational results of security control implementation. Once security is integrated into an organization's processes, the processes become self-regenerating, measurement data collection becomes fully automated, and the mission or business impact of security-related actions and events can be determined by data correlation analysis. Appendix A contains examples of implementation, and efficiency and effectiveness metrics, based on NIST SP 800-26 critical elements.

The metrics at Level 4 and Level 5 concentrate on measuring effectiveness and efficiency of implemented security controls and the impact of these controls on the organization's mission. These metrics concentrate on the evidence and results of testing and integration. Instead of measuring the percentage of approved security plans, these metrics concentrate on validating whether security controls, described in the security plans, are effective in protecting the organization's assets. For example, computing the percentage of crackable passwords within a predefined time threshold will validate the effectiveness of an organization's password policy by measuring the length of time required to break policy-compliant passwords. The impact metrics would quantify incidents by type (e.g., root compromise, password compromise, malicious code, denial of service) and correlate the incident data to the percentage of trained users and system administrators to measure the impact of training on security.

3.4 Success Factors

A number of factors influence the success of an IT security metrics program. Success is achieved only if the program is organized and implemented with the consideration of specific organizational structure, processes, and within reasonable resource constraints.

3.4.1 Organizational Considerations

System stakeholders must be included in the IT security metrics development and program implementation. Organizational elements that do not have IT security as their primary responsibility but interact with IT security on a regular basis (e.g., training, resource management, legal department) must also be included in this process. If an organizational element exists that is responsible for performance measurement in general, the development and implementation of an IT security metrics program should be coordinated with that organization. If a process exists for approving organization wide data calls and actions, the IT security metrics program development and implementation should comply with the existing process.

3.4.2 Manageability

A very important success factor is manageability of the metrics program. Results of many security activities can be quantified and used for performance measurement; however, since resources are limited and the majority of resources should be applied to correcting performance gaps, organizations should prioritize measurement requirements to ensure that a limited number of metrics are gathered. This number should be kept between five and ten metrics per stakeholder at a single time. As the program matures and target levels of measurement are reached, obsolete metrics should be phased out, and the new metrics that are measuring completion and effectiveness of more current items should be deployed. New metrics will also be required if the mission of the organization is redefined or if there are changes in security policies and guidance.

3.4.3 Data Management Concerns

To ascertain the quality and validity of data, data collection methods and data repositories used for metrics data collection and reporting, either directly or as data sources, should be standardized. The validity of data is suspect if the primary data source is an incident-reporting database that stores only the information reported by some organizational elements, or if reporting processes between organizations are inconsistent. The importance of standardizing reporting processes cannot be overemphasized. When organizations are developing and implementing processes that may serve as inputs into an IT security metrics program, they must ensure that data gathering and reporting are clearly defined to facilitate the collection of valid data.

Finally, organizations must understand that although they may collect a lot of IT security data, not all data will be useful for their metrics program at any given point in time. Any data collection, specifically for the purpose of IT security metrics, must be as nonintrusive as possible

and of maximum usefulness to ensure that available resources are primarily used to correct problems, not collect data. The establishment of a metrics program will require a substantial investment to ensure that the program is properly implemented to maximize its benefits. The resources required for maintaining the program are not expected to be as significant.

4. METRICS DEVELOPMENT AND IMPLEMENTATION APPROACH

Two processes guide the establishment and operation of an IT security metrics program: metrics development and metrics implementation. The metrics development process establishes the initial set of metrics and selection of the metrics subset appropriate for an organization at a given time. The metrics program implementation process operates a metrics program that is iterative by nature and ensures that appropriate aspects of IT security are measured for a specific time period. The remainder of this section describes the metrics development process. Section 5 describes the metrics program implementation process.

4.1 Metrics Development Process

Figure 4-1 illustrates the place of IT security metrics within a larger organizational context and demonstrates that IT security metrics can be used to progressively measure implementation, efficiency, effectiveness, and the business impact of IT security activities within organizations or for specific systems.

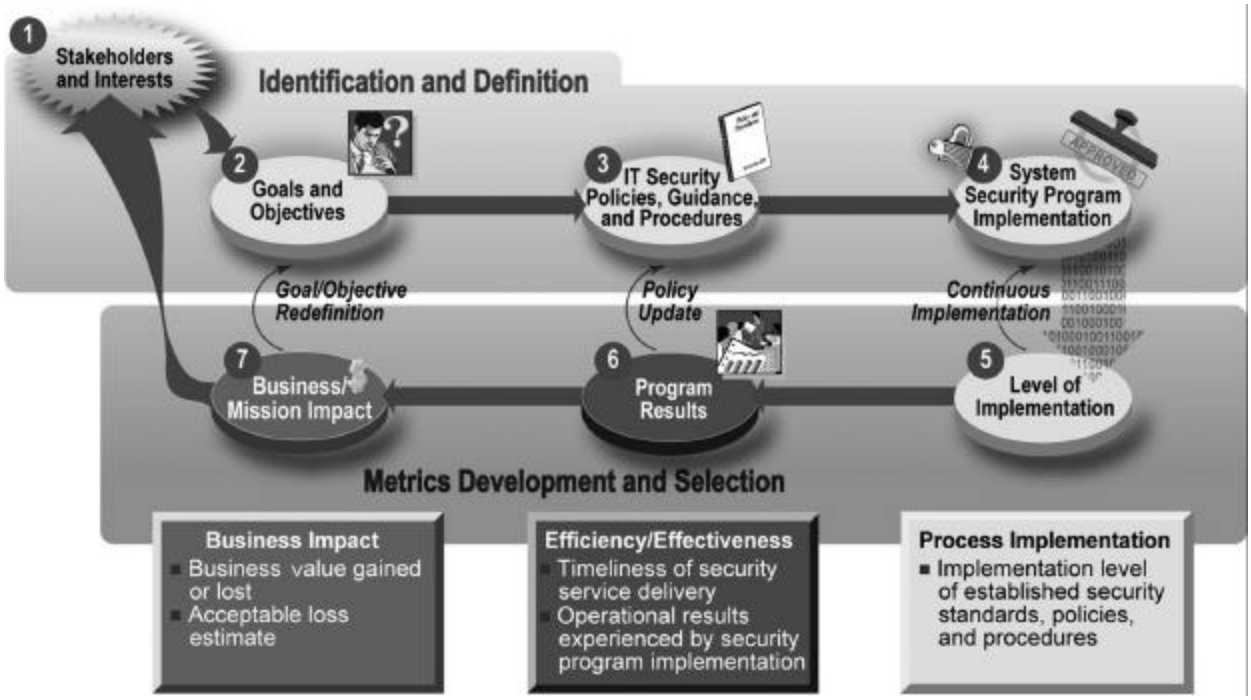

Figure 4-1. IT Security Metrics Development Process

The IT security metrics development process consists of two major activities:

1. Identification and definition of the current IT security program; and
2. Development and selection of specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls.

The process steps do not need to be sequential. Rather, the process illustrated in Figure 4-1 provides a framework for thinking about metrics and facilitates the identification of metrics to be developed for each system. The type of metric depends on where the system is within its life cycle and the maturity of the IT system security program. This framework facilitates tailoring metrics to a specific organization and to the different stakeholder groups present within each organization.

4.1.1 Stakeholder Interest Identification

In Phase 1 of the metrics development process (see Figure 4-1), anyone within an organization should be an IT security stakeholder, though some functions have a greater stake in security than others. The primary IT security stakeholders are?

- Head of Agency
- Chief Information Officer (CIO)
- Security Program Manager/Information System Security Officer (ISSO)
- Program Manager/System Owner
- System Security Officer
- System Administrator/Network Administrator
- IT Support Personnel.

The secondary security stakeholders are members of organizational entities that do not have security as their primary mission but touch security in some aspects of their operations. Examples of secondary security stakeholders include?

- Chief Financial Officer (CFO)
- Training Organization
- Human Resources/Personnel Organization
- Inspectors General (IG).

The interests of each stakeholder will differ, depending on the security aspects of their role and on their position within the organizational hierarchy. Each stakeholder may require an additional set of customized metrics that provides a view of the organization's IT security performance within their area of responsibility. Stakeholder interests may be determined through multiple venues, such as interviews, brainstorming sessions, and mission statement reviews. The total number of metrics should be between five and ten for each individual stakeholder. It is recommended that fewer metrics per stakeholder be used when an organization is establishing a

security program; the number of metrics per stakeholder will increase gradually with the maturity of the IT security program and of the metrics program.

Stakeholders should be involved in each step of security metrics development to ensure organizational buy-in to the concept of measuring security performance. Stakeholder involvement will also ensure that the sense of ownership of the system security metrics exists at multiple levels of the organization to encourage the overall success of the program.

The four measurable aspects of IT security (business input, efficiency, effectiveness, and implementation) speak to different stakeholders. While an executive will be interested in the business and mission impact of IT security activities (e.g., what is the monetary and public trust cost of the latest incident or is there an article about us in a major newspaper?), security and program managers will be interested in the effectiveness and efficiency of IT security programs (e.g., could we have prevented the incident and how fast did we respond to it?), and the system or network administrators will want to know what went wrong (e.g., have we performed all necessary steps to avoid or minimize the impact of the incident?).

4.1.2 Goals and Objectives Definition

Phase 2 of the metrics development process (see Figure 4-1) is to identify and document system security performance goals and objectives that would guide security control implementation for that system. System security goals and objectives for federal government systems are expressed in the form of high-level policies and requirements, laws, regulations, policies, and guidance, including?

- Clinger-Cohen Act
- Presidential Decision Directives
- FISMA
- OMB Circular A-130, Appendix III
- NIST Federal Information Processing Standards (FIPS) and Special Publications.

The sample metrics contained in Appendix A use the NIST 800-26 critical elements and subordinate questions as specific security performance goals and objectives, respectively. However, other documents can be used as sources of applicable system security goals and objectives, when appropriate.

Applicable documents should be reviewed to identify and extract applicable security performance goals and objectives. The extracted goals and objectives should be validated with the organizational stakeholders to ensure stakeholder acceptance and participation in the metrics development process. Appendix A provides samples of IT security metrics with corresponding goals and objectives.

4.1.3 IT Security Policies, Guidance, and Procedures Review

The details of how security controls should be implemented are usually described in organization-specific policies and procedures (Phase 3) that define a baseline of security practices that are prescribed for the system. Specifically, they describe security control objectives and techniques that should lead to accomplishing system security performance goals and objectives. These documents should be examined during initial development and in future metrics development when the initial list of metrics is exhausted and needs to be replaced with other metrics. The applicable documents should be reviewed to identify prescribed practices, applicable targets of performance, and detailed security controls for system operations and maintenance.

4.1.4 System Security Program Implementation Review

In Phase 4 of the metrics development process (see Figure 4-1), any existing metrics and data repositories that can be used to derive metrics data should be reviewed. Following the review, applicable information should be extracted and used to identify appropriate implementation evidence that will support metrics development and data collection. Implementation evidence points to aspects of IT security controls that would be indicative of the security performance objective being met, or at least that actions leading to the accomplishment of the performance objective in the future are performed. The system security requirements, processes, and procedures that have been implemented can be extracted by consulting multiple sources, including documents, interviews, and observation. The following sources may contain information from which metrics data can be generated:

- System Security Plans
- FISMA OMB Plan of Actions and Milestones (POA&M) reports
- Latest GAO and IG findings
- Tracking of security-related activities, such as incident handling and reporting, testing, network management, audit logs, and network and system billing
- Risk assessments and penetration testing results
- C&A documentation (e.g., security test and evaluation [ST&E] reports)
- Contingency Plans
- Configuration Management Plans
- Training results and statistics.

As system security practices evolve and the documents describing them change, the existing metrics will be retired and new metrics developed. To ensure that the newly developed metrics

are appropriate, these documents and other similar documents will need to be examined to identify new areas to be captured in metrics.

4.1.5 Metrics Development and Selection

Phases 5, 6, and 7, depicted in Figure 4-1, involve developing metrics that measure process implementation, effectiveness and efficiency, and mission impact. The specific aspect of IT security that metrics will focus on at a given point in time will depend on the security effectiveness level, as defined in NIST SP 800-26. Appendix A, Sample IT Security Metrics, suggests measures that can be implemented based on the critical elements contained in the 17 IT security topic areas. Implementation evidence, required to prove higher levels of effectiveness, will change from establishing existence of policy and procedures, to quantifying implementation of these policies and procedures, then to quantifying results of implementation of policies and procedures, and ultimately, to identifying impact of implementation on the organization's mission.

The universe of possible metrics, based on existing policies and procedures, will be quite large. Metrics must be prioritized to ensure that the final set selected for initial implementation has the following qualities:

- Facilitates improvement of high-priority security control implementation. High priority may be defined by the latest GAO or IG reports, results of a risk assessment, or internal organizational goal.

- Uses data that can realistically be obtained from existing processes and data repositories.

- Measures processes that already exist and are relatively stable. Measuring nonexistent or unstable processes will not provide meaningful information about security performance and will therefore not be useful for targeting specific aspects of performance. On the other hand, attempting such measurement may not be entirely useless, because such a metric will certainly produce poor results and will therefore identify an area that requires improvement.

Agencies may decide to use a weighting scale to differentiate importance of selected metrics and to ensure that the results accurately reflect existing security program priorities. This would involve assigning values to each metric based on the importance of a metric in the context of the overall security program. Metrics weighting should be based on the overall risk mitigation goals and is likely to reflect higher criticality of department-level initiatives versus smaller scale initiatives and is a useful tool that facilitates integration of IT security metrics into the departmental capital planning process.

A phased approach may be required to identify short-, mid-, and long-term metrics in which the implementation time frame depends on a combination of system-level effectiveness, metric priority, data availability, and process stability. Once applicable metrics that contain the qualities described above are identified, they will need to be documented in the Metric Detail Form in Table 4-1.

Performance Goal	State the desired results of implementing one or several system security control objectives/techniques that are measured by the metric. When using NIST SP 800-26, this item will list a critical element, as stated in 800-26.
Performance Objective[3]	State the actions that are required to accomplish the performance goal. When using NIST SP 800-26, this item will list one or more subordinate questions, as stated in 800-26. Multiple performance objectives can correspond to a single performance goal.
Metric	Define the metric by describing the quantitative measurement(s) provided by the metric. Use a numeric statement that begins with the words "percentage," "number," "frequency," "average," or other similar terms.
Purpose	Describe the overall functionality obtained by collecting the metric. Include whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items.
Implementation Evidence	List proof of the security controls' existence that validates implementation. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric. (Sections 4.1.3, IT Security Policies, Guidance, and Procedures Review; 4.1.4, System Security Program Implementation Review; and 4.1.5, Metrics Development and Selection, contain a discussion of what information can be used to identify appropriate implementation evidence for individual metrics. Section 5.2, Collect Data and Analyze Results, contains a discussion and a list of common causation factors.)
Frequency	Propose time periods for collection of data that is used for measuring changes over time. Suggest time periods based on likely updates occurring in the control implementation. (Section 4.3, Feedback Within Metrics Development Process, contains a discussion on the frequency of metric data collection.)
Formula	Describe the calculation to be performed that results in a numeric expression of a metric. The information gathered through listing implementation evidence serves as an input into the formula for calculating the metric.
Data Source	List the location of the data to be used in calculating the metric. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information. (Section 3.4.3, Data Management Concerns, contains a discussion on metrics data sources.)
Indicators	Provide information about the meaning of the metric and its performance trend. Propose possible causes of trends identified through measurement and point at possible solutions to correct the observed shortcomings. State the performance target if it has been set for the metric and indicate what trends would be considered positive in relation to the performance target. (Section 4.2, Establishing Performance Targets, contains a discussion about the relationship of performance targets and the indicators.) Describe how the information gathered through listing implementation evidence is to be used as input into the analysis of indicators. The implementation evidence serves for validating performance of security activities and pinpointing causation factors.

Table 4-1. Metric Detail Form

[3] When using NIST SP 800-26 subordinate questions, more than one subordinate question can be handled within a single metric.

4.2 Establishing Performance Targets

After applicable metrics are identified and described, performance targets should be identified in the indicator line of the metric form. Performance targets establish a goal by which success is measured. The degree of success is based on the metric result's proximity to the stated performance target. The mechanics of establishing performance targets differ for implementation metrics and the other three types of metrics (effectiveness, efficiency, and impact). For implementation metrics, targets are set to 100 percent completion of specific tasks. When implementation metrics that correspond to all NIST SP 800-26 critical elements reach the target of 100 percent completion, the organization has reached Level 3, depicted in Figure 3-1.

Setting performance targets for efficiency, effectiveness, and impact metrics is more complex, because these aspects of security operation do not assume a specific level of performance. Management will need to apply qualitative and subjective reasoning to determine appropriate levels of security effectiveness and efficiency and to use these levels as targets of performance for applicable metrics. Although all organizations desire effective implementation of security controls, efficient delivery of security services, and minimal impact of security events on its mission, the associated measurements will be different for different systems. An organization can attempt to establish performance targets for these metrics and should be ready to adjust these targets, based on actual measurements, once they are obtained. The organization may also decide not to set targets for these metrics until the first measurement is collected that can be used as a performance baseline. Once the baseline is obtained and corrective actions identified, appropriate measurement targets and implementation milestones can be defined that are realistic for a specific system environment. If performance targets cannot be established after the baseline has been obtained, management should evaluate whether the measured activities and corresponding metrics are providing expected value for the organization.

Establishment of effectiveness, efficiency, and impact metrics baselines and targets of performance can be facilitated if historic data that pertains to these metrics is available. Trends observed in the past will provide insight into ranges of performance that have existed previously and guide the creation of realistic targets for the future. In the future, expert recommendations and standards within the industry may provide a means of setting targets when these are published. Figure 4-2 provides an example of an IT security metric trend, based on the percentage of approved security plans.

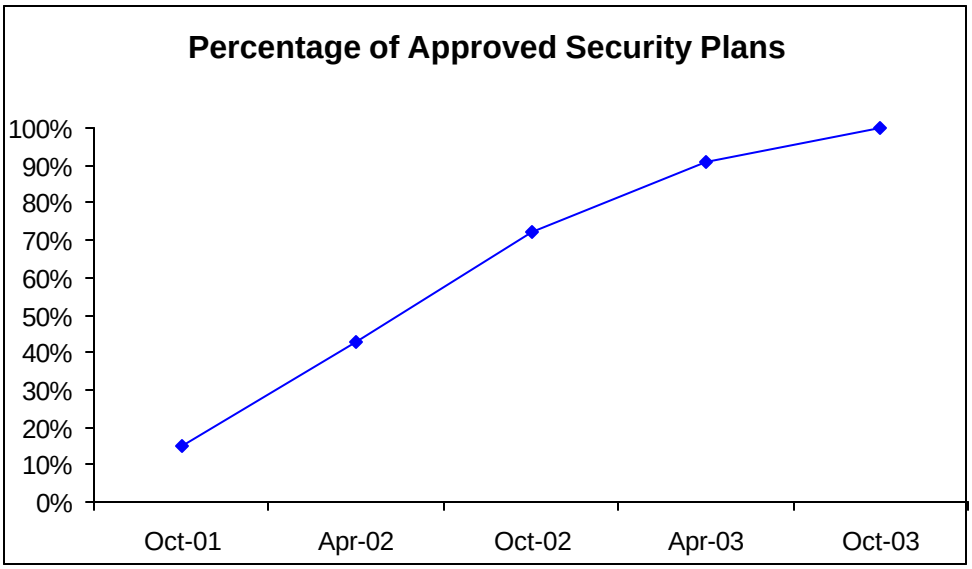

Figure 4-2. IT Security Metric Trend Example

4.3 Feedback Within Metrics Development Process

The metrics that are ultimately selected for implementation will be useful not only for measuring performance, identifying causes of unsatisfactory measurements, and pinpointing improvement areas, but also for facilitating continuous policy implementation, effecting security policy changes, and redefining goals and objectives. This relationship is depicted by the feedback arrows in Figure 4-1, which are marked as Goal/Objective Redefinition, Policy Update, and Continuous Implementation. Once the measurement of security control implementation commences, subsequent measurements can be used to identify performance trends and ascertain whether the rate of implementation is appropriate. A specific frequency of each metric collection will depend on the life cycle of a measured event. A metric that pertains to the percentage of completed or updated security plans should not be collected more often than semiannually. A metric that pertains to crackable passwords should be collected at least monthly. Continuous measurement will point to continuous implementation of applicable security controls. Once effectiveness and efficiency metrics are implemented, they will facilitate an understanding of whether the security control performance goals, set in the security policies and procedures, are realistic and appropriate.

For example, if a security policy defines a specific password configuration, compliance with this policy could be determined by measuring the percent of passwords that are configured according to the policy. This measure addresses the level of security control implementation. It is assumed that configuring all passwords according to the policy will significantly reduce, if not eliminate, system compromises through broken passwords. To measure effectiveness of the existing password policy implementation, the percent of crackable passwords (by common password-breaking tools) could be identified. This measure addresses the effectiveness of the security

control as implemented. If a significant percent of crackable passwords remain after the required password policy has been implemented, the logical conclusion is that the underlying policy may be ineffective in thwarting password compromises. If so, an organization will need to consider strengthening the policy or implementing some other mitigating measures. An organization will then need to determine costs and benefits of keeping the password policy as is, tightening it, or replacing password authentication with other techniques. Conducting cost-benefit analyses will generate business impact metrics that will address the issue of redefining system identification and authentication objectives and appropriately realigning these objectives with the system mission.

5. METRICS PROGRAM IMPLEMENTATION

Implementation of IT security metrics involves using IT security metrics for monitoring IT security control performance and using the results of the monitoring to initiate performance improvement actions. The iterative process consists of six phases, which, when fully executed, will ensure continuous use of IT security metrics for security control performance monitoring and improvement. The IT security metrics program implementation process is depicted in Figure 5-1.

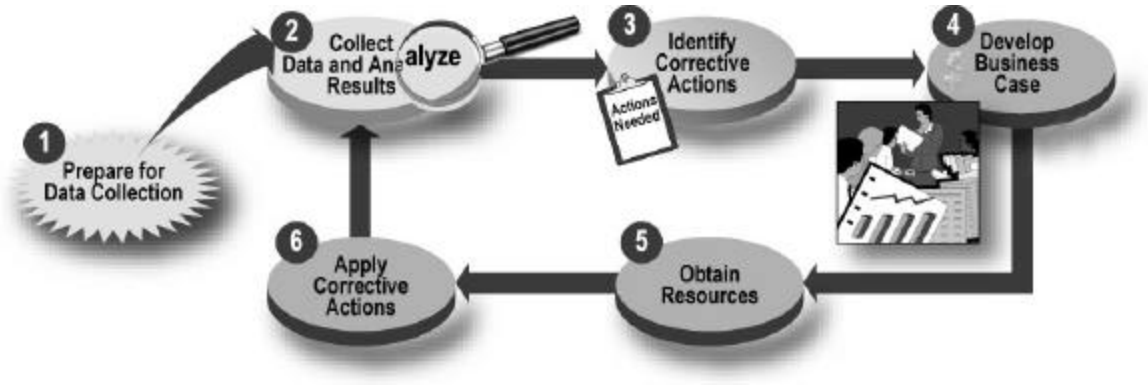

Figure 5-1. IT Security Metrics Program Implementation Process

5.1 Prepare for Data Collection

Phase 1 of the process, *Prepare for Data Collection*, involves activities that are key for establishing a comprehensive IT security metrics program, including the IT security metrics identification, definition, development, and selection activities, described in Section 4.1, and developing a metrics program implementation plan.

After the metrics have been identified, specific implementation steps should be defined on how to collect, analyze, and report the metrics. These steps should be documented in the Metrics Program Implementation Plan. The following items may be included in the plan:

- Metrics roles and responsibilities, including responsibilities for data collection (both soliciting and submitting), analysis, and reporting
- Audience for the plan
- Process of metrics collection, analysis, and reporting, tailored to the specific organizational structure, processes, policies, and procedures
- Details of coordination within the Office of the CIO, such as with risk assessment, C&A, and FISMA reporting activities

- Details of coordination between the Office of the CIO and other functions within the agency, external to the CIO (e.g., information assurance [IA], if it is separate from the CIO; physical security; personnel security; and critical infrastructure protection [CIP]) to ensure the metrics data collection is streamlined and nonintrusive
- Creation or selection of data collection and tracking tools
- Modifications of data collection and tracking tools
- Metrics summary reporting formats.

5.2 Collect Data and Analyze Results

Phase 2 of the process, *Collect Data and Analyze Results*, involves activities that are essential for ensuring that the collected metrics are used to gain an understanding of system security and to identify appropriate improvement actions. This phase includes the following activities:

- Collect metrics data, according to the processes defined in the Metrics Program Implementation Plan
- Consolidate collected data and store in a format conducive to data analysis and reporting, for example, in a database or a spreadsheet
- Conduct gap analysis - compare collected measurements with targets, if defined, and identify gaps between actual and desired performance
- Identify causes of poor performance
- Identify areas requiring improvement.

The causes of poor performance can often be identified using the data from more than one metric. For example, determining that the percentage of approved security plans is unacceptably low would not be helpful for determining how to correct the problem. To determine the cause of low compliance, information will need to be collected regarding the reasons for low percentages (e.g., lack of guidance, insufficient expertise, or conflicting priorities). This information can be collected as separate metrics or as implementation evidence for the percentage of approved security plans. Once this information is collected and compiled, corrective actions could be targeted at the cause of the problem.

The following are examples of causation factors, contributing to poor security control implementation and effectiveness:

- Resources - Insufficient human, monetary, or other resources
- Training - Lack of appropriate training for the personnel installing, administering, maintaining, or using the systems

- System Upgrades - Security patches that have been removed but not replaced during the operating system upgrades

- Configuration Management Practices - New or upgraded systems that are not configured with required security settings and patches

- Software Compatibility - Security patches or upgrades that are incompatible with software applications supported by the system

- Awareness and Commitment - Lack of management awareness and/or commitment to security

- Policies and Procedures - Lack of policies and procedures that are required to ensure existence, use, and audit of required security functions

- Architectures - Poor system and security architectures that make systems vulnerable

- Inefficient processes - Inefficient planning processes that influence the metrics (including communication processes necessary to direct organizational actions).

5.3 Identify Corrective Actions

Phase 3 of the process, *Identify Corrective Actions*, involves the development of a plan that will provide the roadmap of how to close the implementation gap identified in Phase 2. This phase includes the following activities:

- Determine range of corrective actions - Based on the results and causation factors, identify corrective actions that could be applied to each performance issue. Corrective actions may include changing system configurations; training security staff, system administrator staff, or regular users; purchasing security tools; changing system architecture; establishing new processes and procedures; and updating security policies.

- Prioritize corrective actions based on overall risk mitigation goals - There may be several corrective actions, applicable to a single performance issue; however, some may be inappropriate if they are inconsistent with the magnitude of the problem or too costly. Applicable corrective actions should be prioritized for each performance issue in the ascending order of cost and descending order of impact. The risk management process, described in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, should be used for prioritizing corrective actions. If weights were assigned to metrics in the Prepare for Data Collection phase, these weights should be used to prioritize corrective actions. Alternatively, weights may be assigned to corrective actions in the Identify Corrective Actions phase based on the criticality of implementing specific corrective actions, cost of corrective actions, and the magnitude of corrective actions' impact on the organization's security posture.

- Select most appropriate corrective actions - Up to three corrective actions from the top of the list of prioritized corrective actions should be selected for conducting a full cost-benefit analysis.

5.4 Develop Business Case and Obtain Resources

Phases 4 and 5, *Develop Business Case* and *Obtain Resources*, respectively, address the budgeting cycle required for obtaining resources required for implementing remediation actions identified in Phase 3. The steps involved in developing a business case are based on industry practices and mandated guidance, including OMB Circular A-11, the Clinger-Cohen Act, and GPRA. The results of the prior three phases will be included in the business case as supporting evidence. The following activities should be performed as a part of business case analysis:

- Document mission and its objectives, identified during Phase 2 of the metrics development process
- Determine the cost of maintaining status quo to use as the baseline for comparing investment alternatives
- Document gaps between target performance and current measurements, identified during Phase 2 of the metrics program implementation process
- Estimate life-cycle cost for each corrective action or investment alternative, identified in Phase 3 of the metrics program implementation process
- Perform sensitivity analysis to discern which variables have the greatest effect on the cost[4]
- Characterize benefits that are quantifiable and nonquantifiable returns that are delivered through improved performance, based on the prioritization of corrective actions performed in Phase 3 of the metrics program implementation process
- Perform risk analysis to take into account the likelihood of obstacles and programmatic risks of a particular alternative
- Prepare budget submission by summarizing key aspects of the business case to accurately depict its merits.

Each agency should follow agency-specific business case guidance during this phase of the process. Typically, the components and analysis of the business will allow an easier completion of internal and external budget requests. A thorough examination of the business case will

[4] If a small change in the value of a variable causes a large change in the calculation result, the result is said to be sensitive to that parameter or assumption.

support and facilitate the obtaining resources process. The obtaining resources phase involves the following activities:

- Responding to budget evaluation inquiries
- Receiving allocated budget
- Prioritizing available resources, assuming that not all requested resources will be allocated
- Assigning resources to perform corrective actions.

5.5 Apply Corrective Actions

Phase 6 of the process, *Apply Corrective Actions*, involves implementing corrective actions in technical, management, and operational areas of security controls. After corrective actions are applied, the cycle completes itself and restarts with a subsequent data collection and analysis. Iterative data collection, analysis, and reporting will track progress of corrective actions, measure improvement, and identify areas for further improvement. The iterative nature of the cycle ensures that the progress is monitored and the corrective actions are affecting system security control implementation in an intended way. Frequent performance measurements will ensure that if corrective actions are not implemented as planned, or if their effect is not as desired, quick course corrections can be made, internally to the organization, therefore avoiding problems being discovered during external audits, C&A efforts, or other similar activities.

APPENDIX A: SAMPLE IT SECURITY METRICS

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems*, identifies 17 Information Technology (IT) security topics that affect the security posture of an organization. This appendix provides an example of each critical element, formatted according to the metrics form introduced in Section 4.1.5. Each metric in this appendix can be used as a stand-alone measure or as part of a set of metrics; if the metrics are used as a set, redundant questions that apply to multiple metrics do not need to be repeated. The metrics can be used as is or customized to measure the effectiveness of the security controls. Many of the sample metrics contain a comment section that suggests ways to change the metrics to gather additional information, or explains why certain questions were asked.

The implementation evidence supporting the metrics in this appendix may be collected at the system level or at the program level. In some samples, the first part of the metric is capturing data at the program level, then specific questions are asked at the system level. This approach is used to show how the metrics can be aggregated. When gathering metric data at the system level, the program-level questions should be omitted or reworded to capture information applicable to a single system. For metrics that ask for a percentage, the result of the formula should be multiplied by a hundred to produce a percentage value.

This appendix includes some metrics that were required by OMB in the 2003 FISMA reporting guidance. Table A-1 provides a quick reference guide for finding specific metrics that directly correspond to the 2003 OMB FISMA guidance questions. Please note that OMB FISMA metrics require both numbers and percentages for some or just numbers for other metrics. While the table lists all metrics as percentages, the raw number answers to the OMB FISMA metrics are contained in numerators and denominators of formulas. The table specifically points out those metrics for which OMB required raw numbers without percentages and states in a few cases whether numerator or denominator of the metric should be used for response.

Critical Element	Metric	OMB Guidance Reference
1.1	Percentage of systems that had formal risk assessments performed and documented	I.C.1.c
2.1	Percentage of total systems for which security controls have been tested and evaluated in the past year	I.C.1.g
3.1	Percentage of total systems that have the costs of their security controls integrated into the life cycle of the system	I.C.1.f
4.1	Percentage of total systems that have been authorized for processing following certification and accreditation	I.C.1.e
5.2	Percentage of current security plans	I.C.1.d
9.2	Percentage of systems that have a contingency plan	I.C.1.h

Critical Element	Metric	OMB Guidance Reference
9.3	Percentage of systems for which contingency plans have been tested in the past year	I.C.1.i
13.1	Percentage of employees with significant security responsibilities who have received specialized training	I.C.3.c (denominator) and I.C.3.d (numerator)
14.1	Percentage of agency components with incident handling and response capability	I.B.8.c (numerator)
14.2	Number of incidents reported externally to FedCIRC or law enforcement	I.B.9.c

Table A-1. OMB FISMA Metrics Reference

A.1 Risk Management

Critical Element	1.1 Is risk periodically assessed?
Subordinate Question	1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities or other conditions change?
Metric	Percentage of systems that had formal risk assessments performed and documented
Purpose	To quantify the number of risk assessments completed in relation to the organization's requirements.
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. Of the systems in your current inventory, how many systems have had risk assessments performed and documented in the following time frames? (Select the nearest time frame for each system; do not count the same system in more than one time frame.) Within past 12 months_____ Within past 2 years_____ Within past 3 years_____ 4. For any system that underwent a risk assessment, list the number of systems after the reason(s) that apply: Scheduled risk assessment_____ Major change in system environment_____ Major change in facilities_____ Change in other conditions (specify) _____ 5. For any system that has not undergone a risk assessment in the past 3 years, list the number of systems after the reason(s) that apply: No policy _____ No resources____ System tier level does not require _____ System previously not defined____ New system _____ Other (specify) _____
Frequency	Semiannually, annually
Formula	At agency level: Sum of risk assessments on file for each time frame (Question 3) / IT systems in inventory (inventory database) (Question 2)[5]

[5] For metrics that ask for a percentage the result of the formula should be multiplied by a hundred to produce a percentage value.

Data Source	Inventory of IT systems that includes all major applications and general support systems; risk assessment repository
Indicators	This metric computes the percentage of systems that have undergone risk assessments over the last three years (which is normally the required maximum time interval for conducting risk assessments). To establish the distribution of time for risk assessment completion, the number of systems listed for each time frame is computed. The total within three years should equal 100 percent of all required systems. Systems that are not receiving regular risk assessments are likely to be exposed to threats. Question 4 is used to validate the reasons for conducting risk assessments and to ensure that all systems are accounted. Question 5 is included to determine the reason risk assessments were not performed. Defining the cause will direct management attention to the appropriate corrective actions. By documenting and tracking these factors, changes can be made to improve performance by updating the security policy, directing resources, or ensuring that new systems are assessed for risk as required.

Comments: A number of additional metrics may be created to ascertain the number of systems that have undergone risk assessments after a major change, a number of systems that have undergone risk assessments during the last year, a number of systems that have undergone risk assessments during the last year after a major change, and others. This information can be tracked separately to ensure that this requirement is met and that system changes are monitored and responded to appropriately in a timely manner. A system may have had a risk assessment within the past two years, but if a major change has occurred since then, an additional risk assessment is required to ensure that information about the system's vulnerabilities and exposure to risk is updated and the risk managed.

Critical Element	1.2 Do program officials understand the risk to systems under their control and determine the acceptable level of risk?
Subordinate Question	1.2.1 Are final risk determinations and related management approvals documented and maintained on file?
Metric	Percentage of systems that have had risk levels reviewed by management
Purpose	To quantify the degree of management involvement in the completion of risk assessments through the review of findings and concurrence or non-concurrence with the findings
Implementation Evidence	1. How many systems are there in your agency (or agency component, as applicable)? _____ 2. How many IT systems have been assessed for risk during the last reporting period? _____. 3. How many risk findings were discovered for all risk assessments conducted in the reporting period? _____ 4. How many risk findings were concurred by management? _____ 5. How many risk findings were non-concurred by management? _____ 6. Are management approvals recorded and tracked? ? Yes ? No
Frequency	Annually, semiannually
Formula	Sum of concurred and non-concurred findings (Question 4 + Question 5) / Total number of findings (Question 3)
Data Source	Inventory of IT systems that includes all major applications and general support systems; risk assessment repository; Plan of Actions and Milestones (POA&M)
Indicators	This metric monitors management involvement in the risk management process. The target for this metric is to have management review and take appropriate actions through concurrence or non-concurrence with 100 percent of the risk findings. Management must ensure that resources are available to implement the required capabilities in order to secure information systems as needed. Through management's acknowledgment of risk and concurrence and non-concurrence with findings, risk findings can be appropriately prioritized to ensure that remedial actions occur as the results of risk assessments are placed into the decision-making process and formally into a POA&M. While non-concurred findings are not likely to be implemented, the fact that management reviewed and non-concurred with the findings demonstrates that management has assessed and knowingly accepted residual risk.

Comments: Questions 1 and 2 are included to determine whether risk findings are formally available for management review. These questions identify the input that will enable management to be involved in the risk management process. Question 6 validates that management approvals are recorded, to help ascertain the reliability of the metric result. Without a formal record, accountability for management's review of and decisions on risk findings is absent.

A.2 Security Controls

Critical Element	2.1 Have the security controls of the system and interconnected systems been reviewed?
Subordinate Question	2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?
Metric	Percentage of total systems for which security controls have been tested and evaluated in the past year
Purpose	To measure level of compliance with requirement for system security control testing
Implementation Evidence	1. Does your agency maintain a current system inventory? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. For how many systems were system security controls tested in the past year? _____ 4. How many systems have used the following testing methods in the past year to evaluate security controls: Automated tools (e.g., password cracking and war dialing) _____ Penetration testing _____ Security test and evaluation (ST&E) _____ System audits _____ Risk assessments _____ Other (specify) _____ 5. How many systems were tested using any of the methods in Question 4 in the following time frames? (Choose the nearest time frame for each system; do not count the same system in more than time fame.) Within the past quarter _____ Within the past 6 months _____ Within the past 12 months _____ 6. Are all testing instances and results recorded? ? Yes ? No

Frequency	Annually
Formula	Number of systems with controls tested (Question 3) / Total number of systems in the inventory (Question 2)
Data Source	OMB Exhibits 53 and 300; budget office; audits; C&A database; automated tool reports; system testing logs/records
Indicators	The percentage trend should increase and approach or equal 100 percent. Overall, it is important that security controls be tested once they are in place to make sure they are working as proposed. As changes occur within the security environment, the necessary controls also may change. To keep the control current and appropriate for the system, regular control testing and evaluation should be conducted.

Comments: This metric determines whether security controls are tested for each system. This data must be gathered from audit results or directly from system owners. Data validity depends on the availability of a data source that can be determined to reliably record when system tests are conducted. Question 6 addresses the existence of a formal record of testing.

Question 4 validates the use of verifiable testing methods. Question 5 determines the actual frequency of testing to view the distribution of testing over time. If policies are in place to designate testing types and frequency for various types of systems, it is advisable to track evidence of testing through a central compliance and results database.

Critical Element	2.2 Does management ensure that corrective actions are effectively implemented?
Subordinate Question	2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action?
Metric	The average time elapsed between vulnerability or weakness discovery and implementation of corrective action
Purpose	Measures the efficiency of closing significant system weaknesses to evaluate the existence, and the timeliness and effectiveness, of a process for implementing corrective actions
Implementation Evidence	1. Do you have a tracking system for weakness discovery and remediation implementation? ? Yes ? No 2. How many system weaknesses were discovered within the reporting period (count all weaknesses that were opened and closed within the reporting period)? ___ 3. How many weaknesses discovered within the reporting period were closed in— 30 days _____ 60 days _____ 90 days _____ 180 days _____ 12 months _____ Remain open _____
Frequency	Quarterly, semiannually, annually
Formula	(Number of weaknesses x 30 + number of weaknesses x 60 + number of weaknesses x 90 + number of weaknesses x 180 + number of weaknesses x 365) (individual answers to Question 3)/ Total number of weaknesses closed (Sum of all answers to Question 3)
Data Source	Plan of Actions and Milestones (POA&M) tracking system
Indicators	A target time must be set for corrective action implementation. Results should be compared to this target. The trend for corrective action implementation/weakness closure should be toward shorter time frames, as management becomes more aware of applicable processes. Also, efficiencies are likely to be gained from the increasing experience of personnel and the institutionalization of a formal remedial action process. It should be noted that some corrective actions may require an extended period of time to implement.

Comments: This metric determines whether weaknesses are being corrected in a timely manner. This data must be gathered from auditing results or from risk assessment findings that are reported in the POA&M. Data validity depends on the availability of a data source that can be determined to reliably record when weaknesses are discovered and resolved. If no data source exists, it will be difficult to set a realistic time frame for corrective action. A baseline time frame should be pilot tested before a specific (target) time frame is set. In addition, if incidents occur as a result of an open weakness, new time frame targets should be established for closing weaknesses of a certain category.

Question 3 is used to identify the time span in which the majority of weaknesses are closed. Even though a few weaknesses may take a longer time to resolve, which will influence the average, the distribution of resolution time for most weaknesses can still provide insight into performance in relation to the targeted time frame. The metric also can be expanded to describe the types of weaknesses and to correlate them with time periods to discover where there is a dependency between a weakness type and an average closure time.

A.3 System Development Life Cycle

Critical Element	3.1 Has a system development life cycle (SDLC) methodology been developed?
Subordinate Question	3.1.2 Does the business case document the resources required for adequately securing the system? 3.1.3 Does the Investment Review Board ensure investment requests include the security resources needed?
Metric	Percentage of systems that have the costs of their security controls integrated into the life cycle of the system
Purpose	To quantify the percentage of systems that are in compliance with the OMB requirement for integrating security costs into the system life cycle
Implementation Evidence	1. How many systems are there in your organization (or agency component, as applicable)? _____ 2. Do you have a formal, documented SDLC? ? Yes ? No 3. If the answer to Question 2 is no, why not? ? Unaware of requirement ? Lack of resources ? Competing priorities ? Other (specify) _____ 4. Does the SDLC track the cost of security controls? ? Yes ? No 5. Does the SDLC process incorporate the cost of security at every step as required? ? Yes ? No 6. How many systems are in or went through the SDLC? ____
Frequency	Annually
Formula	Number of systems that have gone through (or are going through) SDLC (Question 6) /Number of systems (Question 1)
Data Source	Budget process data (OMB Exhibit 300); review of security plans
Indicators	The goal for this metric is to show an upward trend. High percentage would show that security resources are allocated for each system during the life cycle.

Comments: The implementation evidence for this metric should provide sufficient information to identify why an SDLC has not been developed in those agencies or agency components that

answer “no” to Question 2. Question 6 provides the number of systems that have been completed or are in the midst of an SDLC. The percentage of systems undergoing or completing an SDLC is calculated by using the formula (Question 6 response divided by response to Question 1). Questions 2, 4, and 5 qualify the organization’s eligibility to report a positive result for this metric. A negative answer to any of these questions makes this metric invalid. Question 4 indicates a possible means of obtaining the cost of security controls.

Critical Element	3.2 Are changes controlled as programs progress through testing to final approval?
Subordinate Question	3.2.5 If security controls were added since development, have the security controls been tested and the system recertified?
Metric	Percentage of systems recertified if security controls are added or modified after the system was developed
Purpose	To measure compliance with a requirement for system review and recertification when security controls are added or modified after the system's development
Implementation Evidence	1. Are system changes documented through a configuration management process? ? Yes ? No 2. Number of systems that have had changes in security controls since development _____ 3. Number of systems with changes in security controls that have been recertified since implementation _____
Frequency	Annually
Formula	Number of systems with security control changes recertified (Question 3) / Number of systems with security control changes since development (Question 2)
Data Source	C&A tracking system; configuration management tracking
Indicators	The result for this metric should increase over time and approach 100 percent. Changes in security controls stand a risk of opening new vulnerabilities and may affect other dependent systems and controls. These changes, if significant, should be checked through a formal recertification process that involves ST&E to ensure that controls are working properly. Without formal processes for checking changes, unknown effects may occur across the system and interconnected systems.

Comments: Question 1 is included to validate that changes to systems are recorded and tracked through a formal process. Without formal tracking, the validity of the metric is suspect.

A.4 Authorize Processing (Certification and Accreditation)

Critical Element	4.1 Has the system been certified/recertified and authorized to process (accredited)?
Subordinate Question	4.1.8 Has management authorized interconnections to all systems including systems owned and operated by another program, agency, organization, or contractor?
Metric	Percentage of total systems that have been authorized for processing following certification and accreditation
Purpose	To determine the percentage of systems that are certified and accredited
Implementation Evidence	1. Does your agency (or agency component, as applicable) maintain a complete and up-to-date inventory of systems? ? Yes ? No 2. Is there a formal C&A process within your agency? ? Yes ? No 3. Is the answer to Question 2 is yes, does the C&A process require management to authorize interconnections to all systems? ? Yes ? No 4. Are interconnections to systems documented? ? Yes ? No 5. How many systems are registered in the system inventory? _____ 6. How many systems have received full C&A? _____
Frequency	Quarterly, semiannually, annually
Formula	Number of systems that have been certified and accredited (Question 6) / Total number of systems (Question 5)
Data Source	System inventory; C&A records
Indicators	This metric measures the existence of, and compliance with, a C&A process. An upward trend for this metric is desirable; the goal is to have 100 percent of systems certified and accredited. C&A shows that the system has been thoroughly assessed for risk, and that an agency official accepts full responsibility for the security of a system.

Comments: The implementation evidence for this metric must be extracted by surveying the record custodians for system inventories and C&A documents or by direct query if these inventories and documents are stored in databases. Questions 3 and 4 are included because it is imperative that the C&A process review the system's interconnections with other systems if the

full scope of the system's potential impact on other systems within the agency is to be assessed. Interconnections should be documented to ensure the traceability and accountability of the information used to evaluate systems for C&A. A negative answer to either of these questions makes this metric invalid.

Critical Element	4.2 Is the system operating on an interim authority to process in accordance with specified authority?
Subordinate Question	4.2.1 Has management initiated prompt action to correct deficiencies?
Metric	Percentage of systems that are operating under an Interim Authority to Operate (IATO)
Purpose	To examine the number of unaccredited systems and systems with IATO
Implementation Evidence	1. Does your agency (or agency component, as applicable) maintain a complete and up-to-date inventory of systems? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component)? _____ 3. How many systems are uncertified? _____ 4. How many of the uncertified systems are operating with an IATO? _____ 5. How many corrective actions for IATO systems were identified as required during the current reporting period? _____ 6. How many corrective actions were implemented during the current reporting period? _____ 7. For IATO systems that have not had corrective actions implemented within six months, list reasons for delay (check all that apply): Insufficient funds Lack of personnel Waiting on delivery of necessary components Competing priorities Waiting for internal approval to complete remedial actions Under Designated Approval Authority (DAA) review Other (specify) _____
Frequency	Quarterly, semiannually, annually
Formula	Number of systems operating with an Interim Authority to Operate (Question 4)/ Total number of systems in inventory (Question 2)

Data Source	Security program manager; certification repository; computer security plans; change management process
Indicators	A downward trend is necessary for this metric, and the goal is to have 0 percent of systems operating with IATO. The higher the number of systems with an IATO and the longer they operate under the provisions of an IATO, the greater a system's exposure to security risks, which must be resolved to achieve full accreditation.

Comments: Questions 1 and 3 validate that the information is available to answer the other questions in the metric. Questions 5 and 6 are included to ensure that management is coordinating activities to correct system deficiencies promptly while an IATO exists. This will provide insight into the full functionality of the entire C&A process. Question 7 is included to determine the cause of delays in implementing necessary changes to achieve full accreditation. Once the causes are determined, appropriate actions can be taken to reduce the delays and achieve full accreditation.

A.5 System Security Plan

Critical Element	5.1 Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?
Subordinate Question	5.1.1 Is the system security plan approved by key affected parties and management?
Metric	Percentage of systems with approved system security plans
Purpose	To measure the degree to which system security plans are approved by management, which implies completion of a plan and the plan's compliance with applicable requirements
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. How many system security plans are completed? ___ 4. How many system security plans contain all of the topics prescribed in NIST SP 800-18? _____ 5. How many system security plans have been approved by management? ____
Frequency	Annually
Formula	Number of approved system security plans (Question 5)/ Total number of systems
Data Source	System inventory and system documentation tracking system (Question 2)
Indicators	The target for this metric is 100 percent. An upward trend in the metric, nearing the 100 percent target, is desirable. The completion of system security plans is a requirement of the OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, Computer Security Act of 1987. System security plans should fully identify and describe the controls in place or planned for the system and should include a list of rules of behavior. Management approval of system security plans indicates that the required elements of an adequate system security plan have been completed to direct appropriate system security.

Comments: Questions 3 and 4 validate the completion of an acceptable system security plan; in addition, they could point to a lack of training for management if the number of system security plans approved by management exceeds the number of system security plans that contain all elements required by NIST SP 800-18.

Critical Element	5.2 Is the plan kept current?
Subordinate Question	5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks?
Metric	Percentage of current security plans
Purpose	To determine the currency of system security plans and to ensure that reviews take place periodically and that the plans are updated as necessary
Implementation Evidence	1. How many systems are there in your agency (or agency component, as applicable)?_____ 2. How many system security plans have been completed? _____ 3. For the reporting period, how many system security plans have been reviewed and updated (if needed) within the following time frames? (Choose nearest time period for each system; do not count plan in more than one time period.) Within past 6 months _____ 6-12 months _____ 1-2 years _____
Frequency	Semiannually, annually
Formula	Sum of numbers of system security plans reviewed and updated (if needed) in each period (Question 3) / Total Number of completed system security plans (Question 2)
Data Source	Inventory of IT systems that includes all major applications and general support systems; NIST SP 800-26 self-assessments; system documentation
Indicators	A target time period should be set in each agency for annual review and update of system security plans. The number for each time period should be totaled and divided by the total number of system security plans. This calculation should meet 100 percent of the requirement. There should be an upward trend toward 100 percent if targets are not met during a specific time frame. The validity of the completed system security plans is ascertained by collecting the information in Metric 5.1.

Comments: This metric can be expanded by adding a question that would determine the reasons for security plans not being reviewed and approved as required.

A.6 Personnel Security

Critical Element	6.1 Are duties separated to ensure least privilege and individual accountability?
Subordinate Question	6.1.3 Are sensitive functions divided among different individuals?
Metric	Percentage of systems compliant with the separation of duties requirement
Purpose	To measure the level of compliance with the separation of duties requirement
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. How many of these systems require in their security plan separation of duties to ensure least privilege and individual accountability? _____ 4. How many of these systems have been validated to enforce this requirement? _____
Frequency	Annually
Formula	Number of systems validated to enforce requirement (Question 4) /Number of systems that formally declare the requirement (Question 3)
Data Source	Risk assessments repository; C&A repository
Indicators	The result for this metric should approach 100 percent to ensure that all systems are actually enforcing the separation of duties requirement. A low percentage indicates high-risk exposure because the same individuals are allowed to perform transactions that require separation of duties.

Comments: Questions 1 and 2 establish the basis for applying this metric. If the number of systems within the agency is unknown, the existence and enforcement of the separation of duties requirement cannot be validated. Question 3, which provides a direct input into the metric calculation, also validates that the separation of duties requirement is formally documented in the security plan.

Critical Element	6.2 Is appropriate background screening for assigned positions completed prior to granting access?
Subordinate Question	6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter?
Metric	Percentage of users with special access to systems who have undergone background evaluations
Purpose	To gauge the degree to which individuals with higher-level access (those who can bypass significant technical and operational controls) are screened before being granted such access
Implementation Evidence	1. Are records kept to identify individuals with higher-level access (those who can bypass significant technical and operational controls) to systems and networks? ? Yes ? No 2. Number of personnel who have special access (i.e., can bypass significant technical and operational controls) to systems ____ 3. Number of personnel with special access to systems who have had background screenings completed_____
Frequency	Semiannually, annually
Formula	Number of users with special access who have had background screenings completed (Question 3) / Number of users with special access to systems (Question 2)
Data Source	Personnel database
Indicators	The target for this metric is 100 percent. A low percentage for personnel with high-level access who have undergone a background screening represents a higher potential risk of security incidents caused by internal personnel, who are the most common source of security breaches.

Comments: The reliability of the information for this metric depends on the establishment of a trusted tracking mechanism that stores information on user privileges and background screening. An additional metric should be collected to gauge the frequency with which these "superusers" undergo background screening to ensure that the most up-to-date information is used to evaluate access levels.

A.7 Physical and Environmental Protection

Critical Element	7.1 Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?
Subordinate Question	7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?
Metric	Percentage of information systems libraries that log the deposits and withdrawals of tapes
Purpose	To determine the level of control exercised by the organization over accumulated data stored on tapes and other storage media and limit access to authorized users
Implementation Evidence	1. How many media libraries exist within the organization? _____ 2. How many of the storage media deposited and checked out are accounted for in logs? _____ 3. How many storage media are checked out by authorized personnel on the access control list? _____ 4. How many libraries log deposited and checked out media? _____
Frequency	Semiannually, annually
Formula	Number of libraries that log checkout and deposit events (Question 4) / Total number of media libraries (Question 1)
Data Source	Media library logs; system librarian; ISSO
Indicators	The target for this metric is 100 percent. A low percentage represents potential risk of data loss from security incidents caused by lack of control of data storage media.

Comments: By establishing the number of data storage media in distribution (Question 2) and verifying that only appropriate personnel have access and are logging the location of the media (Question 3), control can be exerted over the withdrawal process for tapes and media.

Critical Element	7.2 Is data protected from interception?
Subordinate Question	7.2.2 Is physical access to data transmission lines controlled?
Metric	Percentage of data transmission facilities in the organization that have restricted access to authorized users
Purpose	To determine what level of control is exercised by the organization over access to data transmission facilities
Implementation Evidence	1. How many telecommunications closets/housings that hold data transmission lines are there within the organization? _____ 2. How many telecommunications closets/housings that hold data transmission lines have physical access restrictions for all points of entry? _____ 3. How many telecommunications closets/housings that hold data transmission lines use the following physical access restrictions? ? Lockable doors ? Keycard/Cipher card control ? Password/Keypad ? Biometrics ? Other (specify) _____ 4. Is there an access control list of personnel authorized to access the telecommunications closets/housings? ? Yes ? No 5. Is there a documented requirement for maintenance or other unauthorized personnel to be accompanied by internal authorized personnel if access is required? ? Yes ? No
Frequency	Semiannually, annually
Formula	Total number of data transmission facilities with physical access restrictions for all points of entry (Question 2) / Total number of telecommunications facilities that house data transmission lines (Question 1)
Data Source	Facility security officers

Indicators	The target for this metric is 100 percent. A low percentage represents greater potential risk from security incidents caused by lack of access control over telecommunications facilities. All points of entry must be restricted to truly safeguard the telecommunications facilities.

Comments: Question 3 is included to determine the strength of the physical restrictions employed. Additional questions could be included to determine the number of telecommunications facilities that use multiple physical restriction mechanisms. Questions 4 and 5 validate the existence and depth of procedures for maintaining an access control list for physical access and the depth of policy/procedures requiring all unauthorized individuals who may access the facility to be accompanied by authorized personnel.

Critical Element	7.3 Are mobile and portable systems protected?
Subordinate Question	7.3.2 Are sensitive data files encrypted on all portable systems?
Metric	Percentage of laptops with encryption capability for sensitive files
Purpose	To determine what level of control is exercised by the organization over access to sensitive information stored on laptops
Implementation Evidence	1. How many laptops exist within the organization? _____ 2. Is there a policy that requires encryption of sensitive data on laptops? ? Yes ? No 3. How many laptops in the organization have encryption software installed? _____ 4. Are laptops periodically reviewed to ensure that sensitive data is encrypted when stored ? Yes No 5. Are all laptop users given training in use of encryption software? ? Yes No
Frequency	Quarterly, semiannually, annually, as determined by the results of laptop audits
Formula	Number of laptops with encryption capability (Question 3) / Total number of laptops (Question 1)
Data Source	Capital asset manager; system inventories; software inventories; security officers; configuration management checklists
Indicators	The target for this metric is 100 percent. A lower percentage represents greater potential risk of data loss caused by lack of encryption on laptops. The review of laptops for encrypted files (Question 4) is useful for ensuring that some level of encryption is occurring and that users are employing the security control. Pinpointing specific files that are sensitive may be too difficult to obtain a precise number.

Comments: Question 2 determines whether a policy has been issued that requires encrypting sensitive files on laptops. Without a documented requirement, implementation of encryption on laptops is less likely. Question 5 is included to determine whether the users understand how to use encryption on laptops. An additional metric will be required to determine whether the encryption capabilities are actually used to encrypt sensitive files stored on laptops.

A.8 Production, Input/Output Controls

Critical Element	8.1 Is there user support?
Subordinate Question	8.1.1 Is there a help desk or group that offers advice?
Metric	Percentage of security-related user issues resolved immediately following the initial call
Purpose	To quantify the rate of security-related user issue resolution by the help desk
Implementation Evidence	1. What is the primary method of direct user support available to answer questions regarding system functionality and system security controls? ? Help desk ? Network administrator ? Security officer ? Other (specify) _____ 2. What are the hours of availability of assistance? ? 24x7 service ? Weekday office hours only ? Weekday office hours plus some weekend and/or evening service 3. Are calls tracked? ? Yes ? No 4. How many security-related problems/trouble tickets were reported during the current reporting period? _____ 5. How many security-related problems/trouble tickets were closed or resolved immediately following the initial call during the current reporting period? _____ 6. Select the most appropriate reason(s) for not resolving security-related issues: ? Lack of help desk staff ? Help desk staff not familiar with security ? High-level subject matter expertise was required 7. When computer security assistance is needed, whom do you call?

	? Help desk ? System/Network administrator ? No one ? Co-worker/Manager
Frequency	Annually, semiannually
Formula	The number of security-related issues resolved (Question 5) / Number of security-related issues reported (Question 4)
Data Source	A survey of several offices, help desk ticket tracking
Indicators	This metric evaluates the effectiveness of help desk activities that are related to security. The metric requires the existence of user support personnel and tracking of issues reported/handled by this group. The percentage of security-related issues resolved immediately following the initial call should increase but realistically will never reach 100 percent because issues that require further assistance will always exist. The rate of resolution indicates the level of help desk staff's proficiency in security-related issues and points at the reasons for the help desk staff's inability to solve the majority of these issues immediately following the initial call.

Comments: Question 1 qualifies the metric. Questions 2 and 3 categorize the availability of support to users. The less support available, the greater the likelihood that security incidents and misconfigurations will go unresolved. Question 6 points at the possible causes for lower than expected results for this metric. Question 7 assesses the extent to which the primary method of user support is actually used

Critical Element	8.2 Are there media controls?
Subordinate Question	8.2.8 Is media sanitized for reuse?
Metric	Percentage of used media sanitized before reuse or disposal
Purpose	To determine whether media controls are being implemented as required by the entire agency or agency component and whether the risk of recovery of sensitive data is reduced by media sanitization
Implementation Evidence	1. Is there a policy for sanitizing media before they are discarded or reused? ? Yes ? No 2. Number of media submitted for disposal or reuse _____ 3. Number of media submitted for disposal or reuse that have been sanitized _____ 4. If all media are not sanitized before being discarded or reused, check all reasons for lack of sanitization: ? Did not know of requirement ? Lack of personnel resources ? Lack of sanitization instructions
Frequency	Annually
Formula	Number of media sanitized (Question 3) / Number of media submitted for reuse or discarding (Question 2)
Data Source	NIST SP 800-26 assessments can provide some level of knowledge of the existence of a sanitization process. To gather the information for the formal metric, a survey would have to be conducted of those responsible for media sanitization. Records may be stored in a media control log or a parts log.
Indicators	The goal is to have 100 percent of media sanitized before reuse or disposal. Without sanitization, elements can be retrieved from the media to allow unauthorized access to information. This risk is reduced through the sanitization process.

Comments: Question 1 is included to determine whether there is a policy concerning sanitization of media to provide direction to personnel. The answer to Question 4 determines why media may not be sanitized prior to being discarded.

A.9 Contingency Planning

Critical Element	9.1 Have the most critical and sensitive operations and their supporting computer resources been identified?
Subordinate Question	9.1.1 Are critical data files and operations identified and the frequency of file backups documented?
Metric	Percentage of critical data files and operations with an established backup frequency
Purpose	To gauge the risk exposure due to insufficient backups
Implementation Evidence	1. Are critical operations and data files identified? ? Yes ? No ? Do not have critical data/operations 2. If the answer to Question 1 is no, why not? ? Did not know of requirement ? Lack of resources ? Other (please explain) 3. Number of critical data files and operations identified as requiring backup _____ 4. Number of critical data files and operations identified as requiring backup for which backup frequency is established and documented _____ 5. Are backups documented? ? Yes ? No 6. Are files backed up regularly (according to requirements)? ? Yes ? No 7. Are backup files tested each time for successful full transfer/copy of data? ? Yes ? No
Frequency	Annually
Formula	Number of critical files with an established backup frequency (Question 4) / Number of critical files requiring backup (Question 3)
Data Source	Answers to NIST SP 800-26 questions and a survey
Indicators	The results of this metric should reach 100 percent indicating that all files requiring backup are being backed up in compliance with an established backup process. Regular backups are the key to information recovery. To achieve a reliable result for this metric, it is first necessary to identify critical files that require backup (Question 1). Then a tracking system must record backups (Question 5).

Comments: Question 6 determines whether backups occur with the required frequency. Lapses in backup time can cause degeneration of original data. Question 7 is asked to determine the quality of the backups. If the integrity of the data is not preserved during backup, there will not be a full recovery when it is necessary to retrieve information from backup sources, rendering the backups ineffective.

Critical Element	9.2 Has a comprehensive contingency plan been developed and documented?
Subordinate Question	9.2.10 Has the contingency plan been distributed to all appropriate personnel?
Metric	Percentage of systems that have a contingency plan
Purpose	To determine the percentage of systems in compliance with the requirement to have a contingency plan. Existence of such a plan indicates a certain level of preparedness if the plan were to be activated.
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. How many systems have a documented contingency plan? _____ 4. How many contingency plans assign responsibilities for recovery? _____ 5. How many contingency plans identify the location of backups? _____ 6. How many contingency plans provide detailed instructions for restoring operations included in the plan? _____ 7. How many contingency plans have been distributed to all appropriate personnel involved with recovery? _____ 8. How many contingency plans have been reviewed and approved by management and key affected parties? _____
Frequency	Annually
Formula	Number of systems with plan (Question 3) / Total number of systems (Question 2)
Data Source	System documentation tracking; NIST self-assessments
Indicators	The desired state for this metric is for 100 percent of systems to have a contingency plan. An upward trend is positive. A low percentage of systems with contingency plans may indicate a lack of an agency policy requiring contingency plans or failure to enforce such a policy.

Comments: Questions 4 through 8 validate that the required major components of a contingency plan are included and that personnel have a copy accessible for use when needed. Question 8 verifies that management has reviewed and approved the contingency plan.

Critical Element	9.3 Are tested contingency/disaster recovery plans in place?
Subordinate Question	9.3.3 Is the plan periodically tested and readjusted as appropriate?
Metric	Percentage of systems for which contingency plans have been tested in the past year
Purpose	To determine the number and percentage of contingency plans tested in the past year
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. How many of the contingency plans have been tested within the last year? _____ 4. Are results of testing recorded? ? Yes ? No 5. How many alterations to the plans were necessary after testing? ____ 6. How many alterations were completed? _____ 7. How many plans were retested after alterations were made? _____ 8. How many plans were finalized and approved by management and affected parties after alterations were made? _____
Frequency	Annually
Formula	Number of contingency plans tested (Question 3) / Number of systems total (Question 2)
Data Source	Contingency plan repository.
Indicators	If this metric yields a low percentage, it identifies specific systems for follow-up and retesting, development of a contingency plan, or analysis of areas in which the contingency plan is not being updated as necessary.

Comments: Questions 4 through 8 validate that results of contingency plan tests are tracked and adjustments made as required. Final approval of contingency plans with changes should require review by management and affected parties to ensure that new procedures and roles are reviewed and understood. This process helps ensure future success in implementing the plan.

The metric's data source portion assumes that there is a contingency plan repository within the agency. If there is a repository, it may be possible to avoid asking implementation evidence

survey questions of specific individuals. If there is no repository, the survey questions will need to be asked of all system owners.

A.10 Hardware and Systems Software Maintenance

Critical Element	10.1 Is access limited to system software and hardware?
Subordinate Question	10.1.1 Are restrictions in place on who performs maintenance and repair activities?
Metric	Percentage of systems that impose restrictions on system maintenance personnel
Purpose	To determine the percentage of systems that have controls on system maintenance activities to limit the risk exposure of data and the possibility of unauthorized installation of components on the system
Implementation Evidence	1. How many systems are there in your agency (or agency component, as applicable)? _____ 2. How many systems have restrictions on who performs maintenance and repair activities on system software and hardware? _____ 3. How many systems log maintenance activities? _____ 4. What documentation outlines maintenance restrictions (check all that apply)? ? System security plan ? IT security policy ? System configuration and operating procedures ? Other (specify) _____ 5. Who is allowed to perform system maintenance and repair (check all that apply)? ? Internal systems engineers ? On site external vendor software or hardware representatives ? Remote external vendor software or hardware representatives ? Other (specify) _____ 6. Are procedures in use to control remote maintenance services when diagnostic procedures or maintenance is performed through telecommunications arrangements? ? Yes ? No
Frequency	Annually
Formula	Number of systems with restrictions on maintenance personnel (Question 2) / Total number of systems (Question 1)

Data Source	Maintenance records; system security and operations documentation
Indicators	This metric seeks to ensure that all systems limit maintenance personnel access to the system. The result should approach 100 percent for full compliance. Maintenance personnel are allowed special access and rights to the system. Without controls on the number of personnel and the type of personnel with maintenance access, the system is more open to unauthorized access to processed and stored data and to the installation of unauthorized components. All systems must have restrictions on maintenance access to reduce exposure to these risks.

Comments: Question 3 is included to determine whether the restrictions that are stated can be verified through stored records regarding access given to system maintenance personnel. Logs can also reveal the number of persons who have maintenance access to the machine, which should be kept to a minimum. Question 4 validates that restrictions are documented. If no documentation exists, each system administrator is less likely to have influence on the control, and there is no continuity as personnel change in the agency, limiting the value of this control significantly. Question 5 seeks to describe the type of personnel who can access the system for maintenance duties. This allows analysis of risk from exposure to external and internal sources. This data also can be used to ensure that compliance measures are in place along with the documented requirements. Question 6 expands on the breadth of the restriction, ensuring that remote access for maintenance activities is formally arranged.

Critical Element	10.2 Are all new and revised hardware and software authorized, tested, and approved before implementation?
Subordinate Question	10.2.3 Are software change request forms used to document requests and related approvals?
Metric	Percentage of software changes documented and approved through change request forms
Purpose	To determine the level of software configuration changes that are documented and approved
Implementation Evidence	1. Do you have a formal process for requesting and tracking software changes on systems and obtaining appropriate approvals for each change (e.g., change request forms)? ? Yes ? No 2. If yes, how do you document changes and approvals? ? Automated system tracks change history and approval ? Change request forms ? Other (specify) _____ 3. Number of software changes or updates that occurred during reporting period_____ 4. Number of changes that have a corresponding documented software change request form/record _____
Frequency	Quarterly, semiannually, annually
Formula	Number of documented approved software changes with forms (Question 4) / Total number of software changes (Question 3)
Data Source	Configuration management database or software change request form documentation
Indicators	The target for the metric is 100 percent. Software changes should be documented and approved as part of a controlled configuration management process. Lack of formal approval requirements for software changes increases the complexity of the version control and security updates that must be applied to a system.

Comments: Questions 1 and 2 are asked to validate that there is a process requiring systematic documentation of requests for software changes and of management approval of these requests.

Critical Element	10.3 Are systems managed to reduce vulnerabilities?
Subordinate Question	10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed?
Metric	Percentage of systems with the latest approved patches installed
Purpose	To quantify the level of risk exposure caused by the lack of current security patch implementation
Implementation Evidence	1. Is regular vulnerability scanning conducted? ? Yes ? No 2. If yes, how many systems are scanned every time? _____ 3. How many of the scanned systems had approved patches? _____ 4. If the answer to Question 1 was no, why not? ? Insufficient funding ? Insufficient staff ? Other (specify) activities had higher priorities ? Other (specify) _____
Frequency	Monthly
Formula	Number of systems with approved patches (Question 3)/ Total number of scanned systems (Question 2)
Data Source	Regular vulnerability scanning results
Indicators	This metric monitors installation of applicable patches and provides useful information about the level of risk exposure at a system level. The goal in this case is 100 percent. The desired trend for this metric is upward.

Comments: This metric counts only those systems where the latest patches were evaluated for impact to system functionality and approved for installation. Without a patch approval process, the impact of patches to systems is unknown and patch application may negatively affect system performance and functionality. Question 4 identifies why a patch compliance validation process may be lacking and points to specific corrective actions that would facilitate establishment of such a process.

A.11 Data Integrity

Critical Element	11.1 Is virus detection and elimination software installed and activated?
Subordinate Question	11.1.1 Are virus scans automatic?
Metric	Percentage of systems with automatic virus definition updates and automatic virus scanning
Purpose	To gauge the degree of protection from known computer viruses
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? ? Yes ? No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. How many systems use automatic virus definition updates and automatic virus scanning? _____ 4. If automatic scanning is performed, in what instances does scanning occur? ? Automatic scan at network login ? Automatic scan at client/server power on ? Automatic scan on diskette insertion ? Automatic scan on download from an unprotected source, such as the Internet ? Automatic network scanning on timed intervals ? Unknown ? Other (specify) _____
Frequency	Semiannually, annually
Formula	Number of systems with automatic virus definition updates and scanning (Question 3) / Number of systems in inventory (Question 2)
Data Source	Survey, network administration records
Indicators	Automatic virus scanning ensures that virus checks are performed at regular intervals. Automatic virus definition updates ensure that the virus checks are performed using the latest virus definition files. The best security practice is to have a 100 percent result for this metric. If a low percentage of systems are using automatic scanning or if user action is required to obtain the latest virus definitions, the risk of systems being infected by computer viruses increases substantially.

Comments: Question 4 validates the use of automatic scanning by specifying when automation occurs. By identifying instances in which automatic scanning does not occur, this question indicates gaps for management to close. If the share of systems using automated virus updates is unknown, the metric result cannot be considered reliable.

Critical Element	11.2 Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?
Subordinate Question	11.2.3 Are procedures in place to determine compliance with password policies?
Metric	Percentage of systems that perform password policy verification
Purpose	To determine whether procedures are performed to ensure that passwords are in compliance with established policies
Implementation Evidence	1. How many systems are there in your agency (or agency component, as applicable) that use passwords? _____ 2. Is a password policy documented? ? Yes ? No 3. If yes, how many systems test passwords for policy compliance? _____ 4. Which of the following methods are used to test passwords for compliance with policy? ? Automatic flagging through policy control software ? Configuration control through software password administration settings ? Password cracking tools ? Manual review of passwords ? Other (specify) _____ 5. If passwords are checked, how often are they assessed (check all that apply)? ? Upon creation ? Weekly ? Monthly ? Quarterly ? Other (specify) _____
Frequency	Semiannually, annually
Formula	Number of systems with password compliance checking (Question 3) / Total number of systems with passwords (Question 1)

Data Source	Survey; risk assessments; query against user password directory or password cracking tool records
Indicators	The target for this metric is 100 percent. First, robust password policies must be in place. Once policies have been established, passwords must be in compliance with these policies to reduce incidents caused by password guessing. Policies should be enforced by an automated or manual methodology.

Comments: Questions 4 and 5 are included to validate that a process is in place for checking password compliance. The type of methodology and its frequency of use indicate the degree of assurance of the consistency and reliability of the process. Manual reviews involve a greater risk of user error; automated methods have greater reliability. In addition, shorter intervals between checks ensure that noncompliant passwords are remedied early, lessening exposure to a security breach through use of a password.

A.12 Documentation

Critical Element	12.1 Is there sufficient documentation explaining how software/hardware is to be used?
Subordinate Question	12.1.3 Is there application documentation for in-house applications?
Metric	Percentage of in-house applications with documentation on file
Purpose	To measure the level of compliance with the requirement for system documentation
Implementation Evidence	1. How many applications are in the inventory? ____ 2. How many applications in the inventory have supporting system documentation on file? _____
Frequency	Annually
Formula	Number of applications with documentation on file (Question2) / Number of applications in inventory (Question 1)
Data Source	Documentation repository/database
Indicators	The target for this metric is 100 percent. A tremendous risk exists when in-house applications are developed, and no system documentation or incomplete documentation exists. Updates and patches have a high probability of being neglected on a system when there is no documentation.

Comments: This metric can be expanded with agency-specific validation questions that address what specific documentation should exist for in-house applications. Depending on the questions, the metric could provide insight into why documentation is not kept (e.g., lack of awareness of location of documentation and lack of an update process). The potential exposure to risk related to the lack of system documentation, such as application manuals, system architecture, and documentation of interconnections with other systems, can also be obtained through specific tailored questions.

Critical Element	12.2 Are there formal security and operational procedures documented?
Subordinate Question	12.2.4 Are there risk assessment reports?
Metric	Percentage of systems with documented risk assessment reports
Purpose	To determine the appropriate documentation of risk assessments for systems
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? ? Yes ? No 2. How many general support systems and major applications are in place as described by NIST SP 800-18? _____ 3. How many of these systems have documented risk assessments? ___ 4. How many risk assessments contain the following information? System characterization (including connections and boundaries)___ Threats identified____ Vulnerabilities identified____ Risk level determined____ Corrective measures outlined____
Frequency	Annually
Formula	Number of systems with documented risk assessments (Question 3) / Total number of systems (Question 2)
Data Source	Risk assessment repository
Indicators	The target for this metric is 100 percent. All required systems must have a documented risk assessment performed at least every three years.

Comments: Question 4 is included for validation of a fully completed risk assessment. All five elements must be present for risk assessment documentation to be in compliance with NIST SP 800-30 guidance. If an element is not accounted for, a risk assessment may be inadequate. This metric can be used to gain further insight into the information provided by Metrics 1.1 and 1.2.

A.13 Security Awareness, Training, and Education

Critical Element	13.1 Have employees received adequate training to fulfill their security responsibilities?
Subordinate Question	13.1.2 Are employee training and professional development documented and monitored?
Metric	Percentage of employees with significant security responsibilities who have received specialized training
Purpose	To gauge the level of expertise among designated security roles and security responsibilities for specific systems within the agency
Implementation Evidence	1. Are significant security responsibilities defined, with qualifications criteria, and documented? ? Yes ? No 2. Are records kept of which employees have specialized security responsibilities? ? Yes ? No 3. How many employees in your agency (or agency component, as applicable) have significant security responsibilities? _____ 4. Are training records maintained? (Training records indicate the training that specific employees have received.) ? Yes ? No 5. Do training plans state that specialized training is necessary? ? Yes ? No 6. How many of those with significant security responsibilities have received the required training stated in their training plan? _____ 7. If all personnel have not received training, state all reasons that apply: ? Insufficient funding ? Insufficient time ? Courses unavailable ? Employee has not registered ? Other (specify) _____
Frequency	Annually, at a minimum

Formula	Number of employees with significant security responsibilities who have received required training (Question 6) / Number of employees with significant security responsibilities (Question 3)
Data Source	Employee training records or database; course completion certificates

Indicators	The target for this measure is 100 percent. If security personnel are not given appropriate training, an organization may not be equipped to combat the latest threats and vulnerabilities. Specific security control options and tools are rapidly changing and evolving. Continued training enforces the availability of necessary security information. This metric can be correlated with the number of security incidents and the number of patched vulnerabilities to determine whether an increase in the number of trained security staff is related to, and facilitates, a reduction in certain types of incidents and open vulnerabilities.

Comments: Questions 1 and 2 are used to gauge the reliability of the information for this metric. Roles and responsibilities must be defined in policy and procedures, and personnel identified to carry out the roles. Questions 4 and 5 provide information to help identify any specialized training that personnel need to complete.

If sufficient training of personnel is not provided, Question 7 helps identify the reason(s). If the cause of insufficient training is known, management can institute corrective actions to remedy this deficiency.

A.14 Incident Response Capability

Critical Element	14.1 Is there a capability to provide help to users when a security incident occurs in the system?
Subordinate Question	14.1.1 Is a formal incident response capability available?
Metric	Percentage of agency components with incident handling and response capability
Purpose	To ensure that there is an agency wide incident response capability
Implementation Evidence	1. Does your agency component maintain an incident response capability? ? Yes ? No 2. If the answer to Question 1 is no, why not? ? Did not know of requirement ? Lack of resources ? Competing priorities 3. Is there a formal process and/or documented incident handling guide that defines "incidents" and describes how to report an incident internally? ? Yes ? No 4. Are incidents monitored and tracked until resolved? ? Yes ? No 5. Are personnel trained to recognize and handle incidents? ? Yes ? No 6. Are alerts and advisories received and responded to? ? Yes ? No 7. Number of incidents reported from your agency component during reporting period_____
Frequency	Semiannually
Formula	Number of agency components that have incident response capability (tally answers to Question 1 from all components) / Total number of components
Data Source	ISSO; NIST SP 800-26 (particularly Items 14.1 and 14.1.1)

Indicators	The goal for this metric is 100 percent; an upward trend is necessary to show progress and the continued strength of the IT security program. The ability to report and handle incidents is critical to maintaining an adequate security posture.

Comments: Question 2 is a causation question that indicates why an agency component's incident response capability may be inadequate. If the answer to Question 2 is "Did not know of requirement," it may be necessary to investigate whether a policy is in place requiring an incident response capability, or if guidance is necessary. Other corrective actions will be required if the answer to Question 2 was "Lack of resources" or "Competing priorities."

Questions 3 through 6 validate that the essential components of an incident response capability are in place and to what degree. For example, if a guide exists but no training is provided to enable personnel to recognize and report incidents, the capability would not be considered robust. The lack of an element in Questions 3 through 6 indicates weakness in the incident response capability that must be addressed to increase functionality and effectiveness.

Question 7 is another validation question. It is unlikely that there will be no incidents reported from an agency component. This number can be compared with agency wide incident reports and correlated with items that would have affected the agency component, to determine whether reporting is occurring as necessary.

Critical Element	14.2 Is incident-related information shared with appropriate organizations?
Subordinate Question	14.2.3 Is incident information reported to Federal Computer Incident Response Center (FedCIRC), National Infrastructure Protection Center (NIPC), and local law enforcement when necessary?
Metric	Number of incidents reported to FedCIRC, NIPC, and local law enforcement
Purpose	To determine the level of appropriate, timely reporting to FedCIRC, NIPC, and local law enforcement
Implementation Evidence	1. Does the agency use a tracking mechanism or database to capture incidents that are required to be reported to FedCIRC, NIPC, and local law enforcement? ? Yes ? No 2. If not, does agency policy state the maximum acceptable time frame for sharing incident information within the agency and with FedCIRC, NIPC, and local law enforcement? ? Yes ? No 3. If the answer to Question 2 is yes, what is the maximum acceptable time listed in agency policy for reporting_____? Within the agency _____ To FedCIRC _____ To NIPC_____ To local law enforcement_____ 4. How many incidents were reported to the following in the current reporting period? Agency____ FedCIRC ____ NIPC____ Local law enforcement____ 5. How many incidents met the required time frame for reporting to the following? Agency____ FedCIRC ____ NIPC____ Local law enforcement____
Frequency	Quarterly, semiannually, annually
Formula	Sum of answers to Question 4
Data Source	Incident reporting database; incident response/reporting policy

Indicators	The ability to complete this metric indicates that the agency's reporting policy is detailed enough to specify an upper limit on the time frame within which incidents are to be reported internally to agency personnel and externally to FedCIRC, NIPC, and local law enforcement. FedCIRC and OMB guidance can be referenced to determine what constitutes a "timely manner," so that the first part of this metric can be answered. Once you have the answer to Question 3, you can compare the average times listed in agency policy with those required in OMB guidance. If the reporting time your agency stipulates is not consistent with OMB guidance, the policy should be modified to comply with the OMB guidance. If there is no agency policy in place, this weakness in the agency IT security program should be corrected.

Comments: Question 1 indicates the level of reliability with which information can be obtained for this metric. If no formal tracking system is used, the validity of the computed number will be suspect. Tracking the timeliness of internal incident reporting within the agency in Questions 4 and 5 can help identify potential causes of delays in external reporting. If internal reporting is slow, external reporting will be affected.

Questions 2 and 3 explore the level of knowledge of what constitutes an appropriate time frame for reporting. These questions aid in determining the reliability of the information collected in Question 5. Compliance cannot be measured unless there is a standard to meet.

A.15 Identification and Authentication

Critical Element	15.1 Are users individually authenticated via passwords, tokens, or other devices?
Subordinate Question	15.1.3 Are vendor-supplied passwords replaced immediately?
Metric	Percentage of systems without active vendor-supplied passwords
Purpose	To determine the percentage of systems that have deleted or replaced vendor-supplied passwords and to gauge level of risk exposure from existing vendor-supplied passwords
Implementation Evidence	1. How many systems do you have within your agency (or agency component)? _____ 2. Is there a documented policy for removing vendor-supplied passwords before software is released into a production environment? ? Yes ? No 3. Are there documented procedures for installing new software that requires vendor-supplied passwords to be changed? ? Yes ? No 4. Are test procedures in place to determine whether vendor-supplied passwords have been replaced before full implementation of software is allowed? ? Yes ? No 5. How many systems actually replace vendor-supplied passwords? _____ 6. Have any system weaknesses been recorded previously related to active vendor-supplied passwords? ? Yes ? No 7. If yes, have these weaknesses been closed and verified? ? Yes ? No
Frequency	Semiannually, annually
Formula	Number of systems with vendor-supplied passwords changed (Question 5) / Total number of systems (Question 1)
Data Source	Risk assessments; ST&E; system audits; baseline security requirements
Indicators	The metric target is 100 percent. All vendor-supplied passwords must be removed to protect systems and applications from unauthorized use.

Comments: Questions 2, 3, and 4 check the reliability of provided information regarding the removal of vendor-supplied passwords. Without a formal policy, it is up to each system administrator to decide about vendor-supplied password removal. These questions also can be used to determine the causes of failure to remove vendor-supplied passwords. Management may need to consider enhancing policies, procedures, and testing processes to promote compliance.

Questions 6 and 7 validate that processes are in place and are effective. System audits and risk assessments will reveal whether there are issues with vendor-supplied passwords. The tracking system for closing such previously identified weaknesses ensures that these issues no longer exist.

Critical Element	15.2 Are access controls enforcing segregation of duties?
Subordinate Question	15.2.1 Does the system correlate actions to users?
Metric	Percentage of unique user IDs
Purpose	To quantify the amount of unique user IDs that trace system events to specific individuals
Implementation Evidence	1. Is each user ID associated with only one unique user? ? Yes ? No 2. Are guest accounts allowed on the system? ? Yes ? No 3. Are access control lists maintained? ? Yes ? No 4. How are user IDs created? ? Randomly by system ? User name variant ? Numerical employee identifier ? Other (specify) _____ 5. How are user IDs checked for uniqueness? ? Automated access control list with duplicate checking ? ID preset as unique ? Manual access control list review ? Other (specify) _____ 6. Are all vendor-supplied user IDs changed? ? Yes ? No 7. How many user IDs are active? _____ 8. How many active user IDs are unique? _____
Frequency	Quarterly, semiannually, annually

Formula	Number of unique IDs (Question 8) / Total number of user IDs (Question 7)
Data Source	Access control list (can sort list if manageable or query for duplicate checking); password files
Indicators	The target for this metric is 100 percent. It is imperative that actions be traced to individuals to maintain control and traceability. Per OMB guidance, "Individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them."

Comments: Questions 1 through 6 are validation questions. The existence of an access control list substantiates that data (in addition to the password files) is available to check for unique user IDs. Allowing guest accounts automatically implies that user actions may not be traceable individually to members of the guest group. The methodology for creating user IDs can ensure the uniqueness of these IDs. Vendor-supplied user IDs should be removed to ensure that unauthorized access does not occur through a vendor-supplied user account that cannot be traced to an individual user.

A.16 Logical Access Controls

Critical Element	16.1 Do the logical access controls restrict users to authorized transactions and functions?
Subordinate Question	16.1.3 Is access to security software restricted to security administrators?
Metric	Percentage of users with access to security software that are not security administrators
Purpose	To determine compliance with policy and the level of risk associated with allowing unauthorized personnel access to security software
Implementation Evidence	1. Is there a policy restricting access to security software to security administrators? ? Yes ? No 2. Do you maintain an access control list? ? Yes ? No 3. Are users designated in the role of security administrator and assigned rights according to data sensitivity? ? Yes ? No 4. Number of users with access to security software_____ 5. Number of security administrators_____ 6. Number of personnel with access to security software who are not identified as security administrators_____
Frequency	Quarterly (if personnel changes are frequent), semiannually, annually
Formula	Number of personnel with access to software who are not identified as security administrators (Question 6) / Number of users with access to security software (Question 4)
Data Source	Access control lists
Indicators	The target for this metric is 0 percent. To ensure that personnel with access to security software have the appropriate skill sets and have undergone appropriate screening, no person should be allowed such access unless they are is designated as a security administrator. The more people have access to security software, the more likely it is that security software misconfigurations or internal security incidents will occur.

Comments: Question 1 is included to determine whether the agency has a policy that provides guidance on specific access restrictions. Once this has been determined, compliance with the policy can be assessed or policies updated. Question 2 determines whether there is a reliable

source of data for the metric. Questions 3 and 5 validate that the agency designates system administrators.

Critical Element	16.2 Are there logical controls over network access?
Subordinate Question	16.2.2 Are insecure protocols disabled?
Metric	Percentage of systems running restricted protocols
Purpose	To determine the security of the system through protocol protection and to gauge the level of risk exposure from allowing prohibited protocols to run on the system
Implementation Evidence	1. How many systems do you have within your agency (or agency component)? _____ 2. Is there a policy regarding individual protocols allowed and disallowed in the environment? ? Yes ? No 3. How many systems are running prohibited protocols? _____ 4. If prohibited protocols are active, why are they enabled? (check all that apply) ? User request ? Functionality requirement ? Legacy system would require massive resources to change ? Waiver received ? Lack of resources ? Lack of system administrator training ? Lack of system administrator time Other (specify) _____
Frequency	Semiannually, annually (also more frequently if automated configuration management/policy enforcement software is in place)
Formula	Number of systems running restricted protocols (Question 3) / Total number of systems (Question 1)
Data Source	Configuration management/enterprise policy software; risk assessments
Indicators	The target is to have 0 percent of systems running restricted protocols. Protocols allow access and transmission of information to occur across systems. Certain protocols contain inherently insecure features and should therefore be largely prohibited. However, port and protocol policies must be set for each agency. Some protocols can be made more secure through enhancements, such as encryption, and

	may not require complete disablement.

Comments: Some insecure protocols may be allowed under certain security enhancement conditions (e.g., adding encryption). A complementary metric may be created to discover whether some protocols are allowed under restricted conditions in the IT security policy. Then, it would be necessary to determine the number of systems employing security enhancements for those protocols. If there are no automated or manual configuration management controls for protocols, assessments can be used to validate that baseline security controls include the restriction of specific protocols.

Question 4 addresses various reasons for allowing prohibited protocols, some of which are totally legitimate. If protocols are allowed for functionality reasons, per user request, or to allow legacy systems to function, they may need to stay open until these reasons are no longer legitimate. If a waiver was obtained, the system must have undergone a formal process by which management accepted responsibility for residual risk caused by keeping the protocols running. The responses, "Lack of resources," "Lack of system administrator training," and "Lack of system administrator time" point to causes that can be alleviated through increased management attention.

Critical Element	16.3 If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?
Subordinate Question	16.3.1 Is a privacy policy posted on the website?
Metric	Percentage of websites with a posted privacy policy
Purpose	To determine the number of agency websites that notify public users of the existence and substance of the agency's privacy policy
Implementation Evidence	1. How many websites are hosted by your agency (or agency component)? _____ 2. What details are contained in the privacy policy about information collected? Use restrictions Access restrictions Retention length ? Disposal practice 3. How many of the websites have a privacy policy publicly posted at the initial access point? _____
Frequency	Quarterly, semiannually, or annually, as needed.
Formula	Websites within the organization with privacy policies posted (Question 4) / Total number of websites hosted by the organization (Question 1)
Data Source	ISSO, webmaster, website review
Indicators	The target for this metric is 100 percent. A lower percentage represents greater potential risk of privacy loss caused by failure to appropriately notify users.

Comments: Question 2 is included to determine the breadth of information contained in the privacy policy. Question 3 assesses the privacy policy's location on websites.

A.17 Audit Trails

Critical Element	17.1 Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?
Subordinate Question	17.1.1 Does the audit trail provide a trace of user actions?
Metric	Percentage of systems on which audit trails provide a trace of user actions
Purpose	To determine compliance with the requirement to correlate user actions on the system in order to maintain traceability
Implementation Evidence	For each system: 1. Is logging activated on the system? ? Yes ? No 2. Do logs capture the user ID for each event? ? Yes ? No 3. Which events do logs record? Successful login ? Yes ? No Failed logins ? Yes ? No Change password ? Yes ? No Unauthorized attempt to access files/directory ? Yes ? No Change access privileges ? Yes ? No Other (specify) _____ 4. Do logs record the following for each event? Date/Time stamp ? Yes ? No User ID ? Yes ? No Type of event ? Yes ? No Command used for event ? Yes ? No
Frequency	Annually
Formula	Number of systems on which logging of user actions is performed (Sum of "Yes" responses to Question 2) / Total number of systems
Data Source	Risk assessment findings; system audits; ST&E; POA&M

Indicators	The target for this metric is 100 percent. It is imperative to trace actions to individuals to maintain control and traceability. According to OMB guidance, "Individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users."

Comments: Questions 1, 3, and 4 seek to validate that logs do capture user IDs for each event. The first step is to ensure that logging is activated. Often, the configuration for logging is not changed from the default setting of "Off." To enable user ID correlation with events, the event types to be captured should be configured. This will allow analysis of user actions as they relate to specific audited events. Logging should include more depth to capture all relevant user activity that could lead to an incident or attempted security breach. Question 4 validates that there is a trace of user action by ID, time of action, and type of action.

APPENDIX B: ACRONYMS

C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
DAA	Designated Approval Authority
FedCIRC	Federal Computer Incident Response Center
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISCAM	Federal Information System Controls Audit Manual
FY	Fiscal Year
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GSS	General Support System
IA	Information Assurance
IATO	Interim Authority to Operate
ID	Identification
IG	Inspector General
ISSEA	International System Security Engineering Association
ISSO	Information System Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
MA	Major Application
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plan of Actions and Milestones
SDLC	System Development Life Cycle
SP	Special Publication
ST&E	Security Test and Evaluation

APPENDIX C: REFERENCES

Bartol N., Givans N., *Measuring the "Goodness" of Security*, 2nd International System Security Engineering Association (ISSEA) Conference Proceedings, February 2001.

Bartol N., *IT Security Performance Measurement: Live*, 3rd ISSEA Conference Proceedings, March 2002

Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759 (Public Law 100-235), January 8, 1988.

E-Government Act of 2002, Title III—Information Security, November 14, 2002.

Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106-398).

General Accounting Office, *Federal Information System Controls Audit Manual (FISCAM)*, GAO/AIMD-12.19.6, January 1996.

Government Information Security Reform Act of 2000.

Government Performance and Results Act of 1993.

National Institute of Standards and Technology, Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology, Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.

National Institute of Standards and Technology, Special Publication 800-18, *Guide for Developing Security Plans and Information Technology Systems,* December 1998.

National Institute of Standards and Technology, Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* August 2001.

National Institute of Standards and Technology, Special Publication 800-30, *Risk Management Guide for Information Technology Systems,* June 2001.

Office of Management and Budget, "Security of Federal Automated Information Resources," Appendix III to OMB Circular A-130, *Management of Federal Information Resources*, February 8, 1996.