The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-55 Revision 1**

Title: **Performance Measurement Guide for Information Security**

Publication Date: **July 2008**

- Final Publication: http://dx.doi.org/10.6028/NIST.SP.800-55r1 (which links to http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf).
- Related Information on CSRC:
  https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final
  https://csrc.nist.gov/publications/detail/sp/800-80/archive/2006-05-04
- Information on other NIST Computer Security Division publications and programs can be found at: https://csrc.nist.gov

The attached publication, Draft SP 800-80, was originally posted for public comment on 5/4/2006. It did not proceed to final publication, and was withdrawn on 11/1/2008; it was superseded by SP 800-55 Revision 1.

The following information was posted with the attached DRAFT document:

May 4, 2006

Draft Special Publication 800-80, Guide for Developing Performance Metrics for Information Security

NIST's Computer Security Division has completed the initial public draft of Special Publication 800-80, *Guide for Developing Performance Metrics for Information Security*.

This guide is intended to assist organizations in developing metrics for an information security program. The methodology links information security program performance to agency performance. It leverages agency-level strategic planning processes and uses security controls from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, to characterize security performance. To facilitate the development and implementation of information security performance metrics, the guide provides templates, including at least one candidate metric for each of the security control families described in NIST SP 800-53.

NIST invites public comments on the draft guideline until 5 p.m. Eastern Daylight Time on June 19, 2006. Written comments on Special Publication 800-88 may be sent to Chief, Computer Security Division, Information Technology Laboratory, Attn: Comments on Draft Special Publication 800-80, NIST, 100 Bureau Dr., Stop 8930, Gaithersburg, Md. 20899-8930. Comments also may be submitted electronically to 800-80comments @ nist.gov

NIST Special Publication 800-80
Initial Public Draft

Guide for Developing Performance Metrics for Information Security

Recommendations of the National Institute of Standards and Technology

Elizabeth Chew
Alicia Clay
Joan Hash
Nadya Bartol
Anthony Brown

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

May 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Reports on Information Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology promotes the United States 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 non-national-security-related information in federal information systems. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, 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, Elizabeth Chew, Alicia Clay, Joan Hash, Nadya Bartol and Anthony Brown, wish to express their thanks to colleagues who reviewed the drafts of this document. In particular, their appreciation goes to Arnold Johnson, Elizabeth Lennon, Lee Imrey, and Linda Duncan, who assisted with our internal review process.

Table of Contents

List of Figures

List of Tables

Executive Summary

This publication focuses on developing and implementing information security metrics for an information security program. The processes and methodologies described in this guidance link information security performance to agency performance by leveraging agency-level strategic planning processes. The performance metrics developed according to this guide will enhance the ability of agencies to respond to a variety of federal government mandates and initiatives, including the Federal Information Security Management Act (FISMA) and the President's Management Agenda (PMA).

The goal of each agency information security program is to provide the appropriate level of protection to the agency's information resources. Information security has become an essential business function, critical to enabling agencies to conduct their operations and deliver services to the public. Each agency's information security program provides direct support to the agency mission. Information security performance metrics provide a means for the monitoring and reporting of agency implementation of security controls. They also help assess the effectiveness of these controls in appropriately protecting agency information resources in support of the agency's mission.

The guide uses security controls, described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* to characterize security performance. It provides at least one candidate metric for each of the 17 control families and offers templates and candidate metrics to facilitate implementation and use of information security performance metrics. The guide describes the information security performance metrics development process as a means for tying information security controls' implementation, efficiency, and effectiveness to an agency's success in its mission-critical activities. This process will assist agency information security practitioners in establishing a direct relationship between program activities under their purview and the agency mission, therefore helping to demonstrate the value of security to their organization.

This guidance document is a companion guide to NIST SP 800-55, *Security Metrics for Information Technology Systems,* using processes and methodologies described in NIST SP 800-55 as a starting point. While focused on NIST SP 800-53 controls, the process described in this guide can be applied to develop agency-specific metrics that may be outside of the scope of SP 800-53.

1. Introduction

Federal agencies are required to collect and report performance metrics and measures to demonstrate compliance with laws and regulations, improve accountability for their programs, and advance efficiencies in delivering programs and services to the public. Information security is one of the functions that agencies are required to report to demonstrate their ability to appropriately protect sensitive and proprietary information that U.S. government systems store, process, and transmit. In addition to regulatory compliance reporting, agencies are using performance metrics and measures as management tools in their internal improvement efforts and linking implementation of their programs to agency-level strategic planning efforts. Information security plays an important role in supporting agency business processes by ensuring secure information technology (IT) infrastructure in support of federal agencies providing services to the public.

1.1 Purpose and Scope

This publication focuses on developing and implementing information security metrics for an information security program. The processes and methodologies described in this guidance link information security performance to agency performance by leveraging agency-level strategic planning processes. By doing so, they help demonstrate how information security contributes to accomplishing agency strategic goals and objectives. The performance metrics developed according to this guide will enhance the ability of agencies to respond to a variety of federal government mandates and initiatives, including the Federal Information Security Management Act (FISMA) and the President's Management Agenda (PMA).

NIST Special Publication (SP) 800-80 expands upon NIST's previous work in the field of security metrics to provide program-level guidance for quantifying information security performance in support of organizational strategic goals. It uses the system security controls, identified in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, as a basis for developing metrics that support the evaluation of security programs. In addition to providing guidance on developing metrics, the guide lists a number of candidate metrics that agencies can tailor, expand, or use as models for developing other metrics. This guidance document is a companion guide to NIST SP 800-55, *Security Metrics for IT Systems*, and uses processes and methodologies described in NIST SP 800-55 as a starting point. While focused on NIST SP 800-53 controls, the process described in this guide can be applied to develop agency-specific metrics that may be outside the scope of NIST SP 800-53.

1.2 Audience

This guide is written primarily for Chief Information Security Officers (CIOs), Senior Agency Information Security Officers (SAISOs), and Information System Security Officers (ISSOs). It targets individuals who are familiar with information security controls as defined in NIST SP 800-53 and those who have knowledge of the basics of information security metrics as described in NIST SP 800-55. The concepts, processes, and candidate metrics presented in this guide can be used within government and industry contexts.

1.3 Relationship to Other NIST Publications

This document focuses on quantifying enterprise and information security program performance. It expands on concepts and processes introduced in NIST SP 800-55 to assist with the

assessment of security program implementation. The metrics development approach described in this guide uses results of a variety of information security activities as sources of data to support information security metrics development, including:

- Security assessment and testing efforts such as those described in NIST Draft SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems;* and
- Metrics and best practices described in NIST publications related to security controls as recommended in NIST SP 800-53.

NIST SP 800-80 differs from NIST SP 800-53A in that it helps quantify implementation and effectiveness of security controls at the information security program level, while NIST SP 800-53A assesses implementation and technical effectiveness of individual controls.

The metrics described in this guide may be used as inputs into the information security program activities described in a number of NIST publications, including:

- Draft NIST SP 800-100, *Information Security Handbook: A Guide for Managers;* and
- NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*.

1.4 Document Organization

The remaining sections of this guide discuss the following:

- Section 2 describes performance metrics-related roles and responsibilities.
- Section 3 identifies performance metrics requirements.
- Section 4 provides an overview of information security performance management.
- Section 5 describes the performance metrics development approach and provides candidate metrics.
- Section 6 concludes the guide.
- Appendix A lists acronyms and abbreviations used in the guide.
- Appendix B lists references used to develop this guide.

2. Roles and Responsibilities[1]

FISMA assigns responsibilities for information security to a number of agency officials. Using these roles and responsibilities as a guideline, this section provides specific guidance on information security performance metrics roles and responsibilities.

2.1 Agency Head[2]

The specific Agency Head responsibilities, related to information security program metrics, are as follows:

- Ensuring that information security metrics are used in support of agency strategic and operational planning processes to secure the organization's mission;
- Ensuring that information security metrics are integrated into annual reporting on the effectiveness of the agency information security program by the CIO;
- Demonstrating support for information security metrics development and implementation and communicating official support to the agency;
- Ensuring that the information security metrics activities have adequate financial and human resources for success;
- Actively promoting information security metrics as an essential facilitator of information security performance improvement throughout the agency; and
- Approving policy to officially institute metrics and initiating the development and implementation of metrics.

2.2 Chief Information Officer

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

- Using information security metrics to assist in monitoring compliance with applicable information security requirements;
- Using information security metrics in annually reporting on the effectiveness of the agency information security program to the agency head;
- Demonstrating management's commitment to information security metrics development and implementation through formal leadership;
- Formally communicating the importance of using information security metrics to monitor the overall health of the information security program and to comply with applicable regulations;
- Ensuring information security metrics program development and implementation;
- Allocating adequate financial and human resources to the metrics program;
- Empowering information security metrics data collection across relevant sources

[1] Public Law 104-106, *Clinger-Cohen Act*, 1996

[2] A full description of agency head, chief information officer, and senior information agency security officer can be found in Draft NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

- Reviewing information security metrics regularly and using information security metrics data to support policy, resource allocation, budget decisions, and provide an understanding of the information security program posture and operational risks to agency systems;
- Ensuring that a process is in place to address issues discovered through metrics analysis and taking corrective actions such as revising security procedures and providing additional security training to staff; and
- Issuing policy, procedures, and guidance to officially develop, implement, and institute metrics.

2.3 Senior Agency Information Security Officer

The SAISO, also known as Chief Information Security Officer (CISO), has the following responsibilities related to information security metrics:

- Integrating information security metrics into the process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;
- Integrating information security metrics in support of the agency CIO's annual reporting to the agency head on the effectiveness of the agency's information security program, including progress of remedial actions;
- Conducting information security metrics development and implementation;
- Ensuring a standard process is used throughout the agency for metrics development, creation, and analysis;
- Leading the development of any internal guidance or policy related to information security metrics;
- Obtaining adequate financial and human resources to support program development and implementation; and
- Using information security metrics for policy, resource allocation, and budget decisions.

2.4 Information System Security Officer

The ISSO has the following responsibilities related to information security metrics:

- Participating in information security metrics program development and implementation by providing feedback on the feasibility of data collection and identifying data sources and repositories; and
- Collecting data or providing metrics data to designated staff that are collecting, analyzing, and reporting the data.

2.5 Other Related Roles

Information security metrics may require inputs from a variety of organizational components, such as incident management information technology operations, enterprise architecture, human resources, physical security, and others. Those personnel have the following responsibilities:

- Participating in information security metrics program development and implementation by providing feedback on the feasibility of data collection and identifying data sources and repositories; and
- Collecting data or providing metrics data to designated staff that are collecting, analyzing, and reporting the data.

3. Legislation and Requirements

This guide focuses on using information security performance metrics to facilitate further integration of information security into agency-level strategic planning and reporting activities. Several pieces of legislation and regulation are driving an increased emphasis on managing, quantifying, and reporting agency performance. The purpose of these efforts is to facilitate streamlining of U.S. government operations, improve efficiencies in delivering services, and demonstrate the value of these services to the public. Agencies are required to strategically plan their initiatives and make these plans and corresponding performance measures or metrics available to the public. Performance metrics, including the ones described in this document, are especially important to these efforts because they:

- Quantify efficiency improvements in service delivery;
- Demonstrate quantifiable progress in accomplishing agency strategic goals and objectives;
- Satisfy legislative requirements;
- Improve accountability for delivering products and services;
- Demonstrate improvement to agency leadership and the general public; and
- Play a key role in initiating improvement actions based on performance trends.

There are two primary laws that govern agency performance measures reporting: the Government Performance Results Act (GPRA) of 1993 and FISMA of 2002. The PMA also addresses this subject. This section provides an overview of GPRA, FISMA, and PMA from the performance measurement point of view and describes their associated performance management requirements.

3.1 Government Performance Results Act

GPRA focuses on improving program efficiency and effectiveness by adequately articulating program goals and providing information on program performance. To structure and facilitate program improvement, it requires agencies to develop multiyear strategic plans and annually report their performance against these plans.

The purpose of GPRA is to:

- Improve the confidence of the American people in the capability of the federal government by systematically holding federal agencies accountable for achieving program results;
- Initiate program performance reform with a series of pilot projects in setting program goals, measuring program performance against those goals, and reporting publicly on their progress;
- Improve federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction;
- Help federal managers improve service delivery by requiring that they plan for meeting program objectives and by providing them with information about program results and service quality;

- Improve Congressional decision making by providing more objective information on achieving statutory objectives and by reporting on the relative effectiveness and efficiency of federal programs and spending; and
- Improve internal management of the federal government.[3]

GPRA mandates agencies to conduct strategic and performance planning, culminating in annual submissions of strategic plans and performance measures reports. GPRA puts strategic and performance planning in the context of the overall agency Capital Planning and Investment Control (CPIC) process by emphasizing "managing for results – what the program accomplishes and how well the accomplishments match with the program's purpose and objectives."[4]

As a part of their annual strategic and performance planning processes, the agencies:

- Define their long-term and annual goals and objectives;
- Set measurable targets of performance; and
- Report their performance against goals and objectives to the Office of Management and Budget (OMB) quarterly.

GPRA is implemented by OMB Circular A-11, *Preparation, Submission, and Execution of the Budget, Part 6.*

3.2 Federal Information Security Management Act

FISMA requires federal agencies to provide appropriate protection of their resources through implementing a comprehensive information security program, commensurate with the sensitivity of the information processed, transmitted, and stored by agency information systems. It also requires agencies to assess and report their performance in implementing and managing information security programs. The purpose of FISMA is to:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets;
- Recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
- Provide for the development and maintenance of minimum controls required to protect federal information and information systems;
- Provide a mechanism for improved oversight of federal agency information security programs;
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense

[3] Public Law 103-62, Government Performance and Results Act of 1993
[4] OMB Circular A-11, Preparation, Submission, and Execution of the Budget, 2005, Section 15, clause 15.5.

and economic security of the nation that are designed, built, and operated by the private sector; and

- Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[5]

FISMA mandates agencies to identify and assess risks to their information security systems and define and implement appropriate security controls to protect their information resources. FISMA requires agencies to report quarterly and annually on the status of their information security programs. Like GPRA, FISMA puts information security in the context of the overall agency CPIC process to ensure that appropriate resources are planned for and allocated to implement required information security controls. OMB publishes annual guidance on the process and elements of annual and quarterly FISMA reporting.

3.3 President's Management Agenda

The PMA, announced in 2001, establishes the President's strategy for improving the management and performance of the federal government. The PMA is guided by three principles: government should be citizen-centered, not bureaucracy-centered; results-oriented; and market-based, actively promoting rather than stifling innovation through competition.

PMA establishes five government-wide initiatives:

1. Strategic management of human capital;
2. Competitive sourcing;
3. Improved financial performance;
4. Expanded electronic government; and
5. Budget and performance integration.

Agencies are required to submit PMA status updates to OMB quarterly. These reports are evaluated and graded according to the Executive Branch Management Scorecard[6] to track how well the agencies are executing the five government-wide management initiatives. Scores for status are based on the Scorecard Standards for Success developed by President's Management Council and have subsequently been refined by incorporating lessons learned through experience in implementing the PMA. The Scorecard Standards for Success lists specific criteria, corresponding to green, yellow, and red colors of the scorecard. Quarterly, OMB assesses each agency's progress in accomplishing deliverables for each of the applicable five initiatives, according to the criteria, and assigns a color grade:

- **Green —** Implementation is proceeding according to plans agreed upon with the agencies.
- **Yellow —** Some slippage or other issues requiring adjustment by the agency in order to achieve the initiative objectives on a timely basis.

[5] Public Law 107-347, E-Government Act of 1992, Title III
[6] http://www.whitehouse.gov/results/agenda/scorecard.html

- **Red —** Initiative in serious jeopardy. Unlikely to realize objectives absent significant management intervention.[7]

Information security is prominently featured in the Scorecard Standards for Success. Agencies are required to report the status of their information security program as a part of their overall PMA report. Furthermore, OMB will not rate agencies as **green** if the agencies do not complete the required criteria.

Section 4 describes how information security performance metrics support the reporting requirements of overall agency performance measures.

[7] http://www.whitehouse.gov/results/agenda/scorecard.html

4. Information Security Performance Management Overview

The goal of each agency information security program is to provide the appropriate level of protection to the agency's information resources. Information security has become an essential business function that is critical to enabling agencies to conduct their operations and deliver services to the public. Each agency's information security program provides direct support to its own mission. This section explains the relationship between overall agency performance measures reporting and information security performance metrics reporting. It also provides agencies with guidance on how to link these two activities to ensure their information security program contributes to the overall accomplishment of the agency mission, goals, and objectives.[8]

4.1 Linkage between Strategic Planning and Information Security

Federal agencies develop their long-term strategic goals as a part of their strategic planning process. Usually, agencies establish approximately five to six strategic goals with several performance objectives describing how each goal will be accomplished. As a part of this process, agencies also develop performance measures to assess accomplishment of their goals and objectives with quarterly and annual performance targets for each performance metric.

FISMA mandated NIST to develop and promulgate standards and guidance pertaining to federal information systems. As a part of this charter, NIST developed and published NIST SP 800-53, which identifies minimum security controls for federal information systems. NIST SP 800-53 organizes these minimum security controls into 17 security control families. Agencies must define and implement the minimum security controls based on sensitivity of data processed, stored, and transmitted on their information systems. As such, agency information security programs must include planning, implementing, monitoring, and reporting on the implementation and effectiveness of these information system security controls.

Information security performance metrics provide a means for the monitoring and reporting of agency implementation of security controls. They also help assess the effectiveness of these controls in appropriately protecting agency information resources in support of the agency's mission. The development and selection of information security performance metrics is similar to that of the performance measures that address agency mission functions, but with some definite differences. Table 1 identifies these similarities and differences and provides examples.

Table 1. Strategic and Information Security Metrics Comparison.

Term	Definition	Examples
Strategic Goal or Strategic Objective	A statement of aim or purpose included in a strategic plan (required under GPRA).	Enhance the use of IT in service delivery and record keeping
Performance Measures[9]	Indicators, statistics, or metrics used to gauge program performance. Used to monitor progress toward accomplishing agency goals and objectives.	Percent of organizations that will use databases, products, or tools to improve quality of service to their constituencies

[8] OMB Circular A-11, Part 6, Section 200, 200.2 provides the definitions for agency goals and objectives. Section 210, 210.1 provides the relationship between the agency mission and its goals.

[9] OMB Circular A-11, Part 6, Section 200, 200.2 provides the definition for performance measures.

Term	Definition	Examples
Information Security Goal	A statement of agency information security requirement or security program goal that will explicitly or implicitly support agency-level strategic goal.	1. All users accessing the organization's systems are uniquely identified and authenticated. 2. Restrict information, system and component access to individuals or machines that are identifiable, known, credible, and authorized.
Information Security Metrics	Monitor and measure implementation and effectiveness of security controls within the context of the security program	1. Percentage of accounts not associated with specific users 2. Percentage of security incidents caused by improperly configured access controls

Ultimately, all agency efforts must support overall agency goals and objectives, which are defined and reassessed annually during agency strategic planning activities. To demonstrate the importance of information security to accomplishing an agency mission, it must be explicitly tied to at least one agency strategic goal or objective as a part of the agency strategic planning processes. This connection can be established by identifying information security goals and objectives that would articulate agency information security requirements within the context of the overall agency mission. Progress toward accomplishing information security goals and objectives may be monitored by implementing appropriate information security performance metrics.

Information security performance metrics can be developed and used at multiple levels within an organization, including the overall agency information security program, operating bureaus' security programs, individual agency programs, or individual agency systems. Information security metrics developed at different levels of an organization should be used for internal management and process improvement purposes, or they may also be aggregated to agency-level information security program performance metrics. Agency-level metrics will either be reported to upper management within an organization or used for external reporting such as agency GPRA and FISMA reporting.

4.2 Security Control Families

To comply with FISMA, agencies are required to implement minimum security controls for their systems, as stated in Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-53. To facilitate explicit linkage of information security activities with agency-level strategic planning, agencies can use specifications for minimum security requirements, as stated in FIPS 200, as an input into objectives for developing information security performance metrics. These specifications, which correspond to the 17 security control families in NIST SP 800-53, are provided below:

- **Access Control (AC):** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

- **Awareness and Training (AT):** Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- **Audit and Accountability (AU):** Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions.
- **Certification, Accreditation, and Security Assessments (CA):** Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- **Configuration Management (CM):** Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.
- **Contingency Planning (CP):** Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
- **Identification and Authentication (IA):** Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- **Incident Response (IR):** Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
- **Maintenance (MA):** Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- **Media Protection (MP):** Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to

authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

- **Physical and Environmental Protection (PE):** Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
- **Planning (PL):** Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
- **Personnel Security (PS):** Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
- **Risk Assessment (RA):** Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
- **System and Services Acquisition (SA):** Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
- **System and Communications Protection (SC):** Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
- **System and Information Integrity (SI):** Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.[10]

Information security performance metrics provide the means for tying information security controls' implementation, efficiency, and effectiveness to an agency's success in its mission-

[10] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.*

critical activities. The performance metrics development process described in this guide will assist agency information security practitioners in establishing a direct relationship between program activities under their purview and the agency mission, therefore helping to demonstrate the value of security to their organization.

5. Performance Metrics Development

Information security metrics used to address information security program performance must be linked to the agency strategic goals and objectives. While the NIST SP 800-55 information security metrics development approach follows this guidance, it applies primarily to the development and use of metrics to measure implementation of security controls for individual systems. NIST SP 800-80 applies this approach to security controls within the context of an information security program.

The subsequent subsections describe the specific approach for developing metrics to measure security control implementation and effectiveness in two different ways—control-specific and cross-cutting. Organizations may elect to use one or both ways to measure performance of their information security program. To select a more appropriate combination of metrics representing both ways of measuring, organizations should consider the following factors:

- Regulatory, legislative, and organizational policy requirements that affect information security requirements, controls, and implementation;
- Agency mission and goals that align with specific agency concerns and risk profile;
- Information security program structure and organization, including distribution of responsibilities for policy development and promulgation, implementation of security controls, and oversight responsibilities; and
- Availability of data that can be used to support measurement.

5.1 Metrics Types

Organizations can use performance metrics to address multiple aspects of their performance. NIST SP 800-55 defines three types of information security metrics and Section 5.4 provides examples of these metrics:

1. Implementation metrics to measure implementation of security policy;
2. Effectiveness/efficiency metrics to measure results of security services delivery; and
3. Impact metrics to measure business or mission impact of security activities and events.

Information security programs can use all three types of metrics; however, the metrics will vary in their usefulness depending on the maturity of each individual information security program. Organizations that are in the process of developing or formalizing their policies and procedures may have a limited ability to collect data to support performance metrics activities. As their information security programs mature to the point where policies and procedures are documented and controls are implemented, data becomes more readily available and can be used to support performance measurement. As more robust, repeatable information security processes are implemented, performance metrics data becomes more reliable and conducive to automation of some or all data collection activities. Higher reliability and availability of data increases the validity of information security performance measures as input into management decision making and process improvement efforts. Figure 2 illustrates the relationship between information security program maturity, ease and means of data collection, and the types of metrics that will be useful and feasible to obtain.

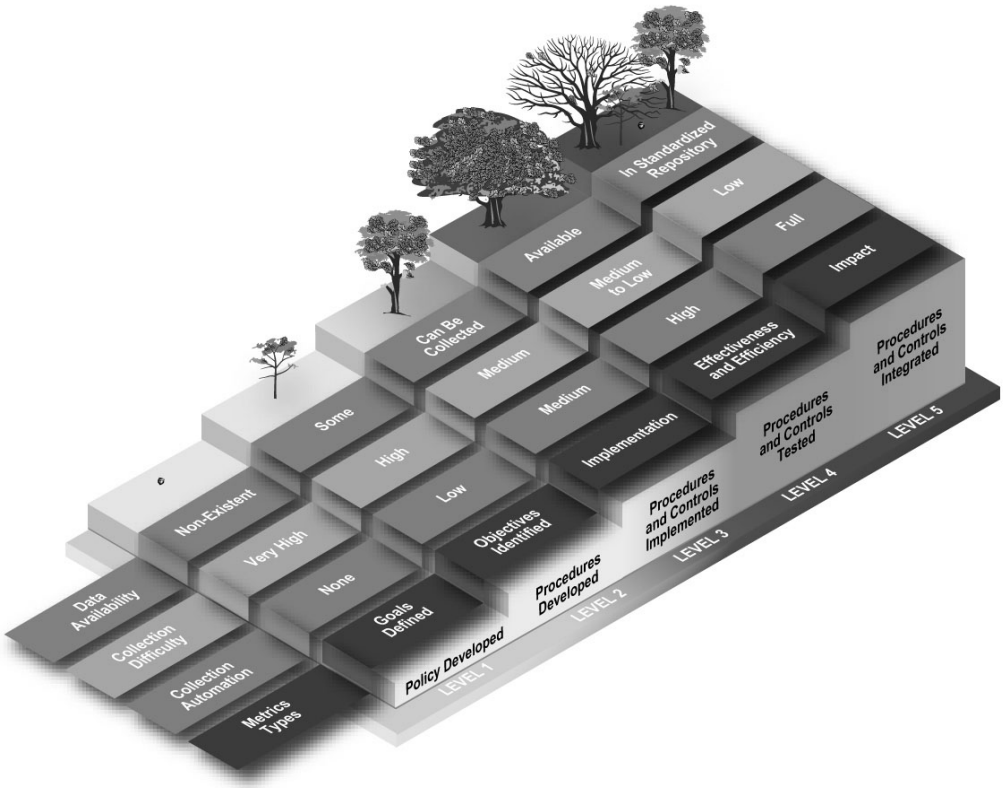

Figure 1. Metrics Within the Context of Information Security Program Maturity[11]

Implementation metrics are used to demonstrate progress in implementing policies and procedures and individual security controls. An example of such a metric would be *percentage of NIST SP 800-53 control families for which policies exist.* Applying security assessment methods described in NIST SP 800-53A and documenting their results will produce data that can be used to quantify the outcomes of applying security controls. Other assessment and testing efforts will also produce useful data. Organizations need this data to support the comprehensive measurement of the effectiveness and efficiency of security control implementation at the security program level. Metrics development and implementation will facilitate linking of this data to agency strategic goals and objectives and demonstrate the impact of information security on the overall strategy implementation. The implementation metrics require data that can be easily obtained from security control assessment reports, FISMA performance measures, plans of actions and milestones (POA&M), and other commonly used means of documenting and tracking information security program activities.

Effectiveness and efficiency metrics are used to monitor results of security control implementation for a single control or across multiple controls. These metrics may require multiple data points quantifying security controls implementation and the results of implementation. For example, *percentage of security incidents caused by improperly configured access controls* relies on information from or about Access Control Policy and Procedures (AC-

[11] NIST SP 800-55 provides a more detailed explanation of this figure.

1); Incident Monitoring (IR-5); Audit Monitoring, Analysis, and Reporting (AU-6); and Monitoring Configuration Changes (CM-4). Effectiveness and efficiency metrics provide key information for information security decision makers about the results of previous policy and acquisition decisions. These metrics can offer insight for improving performance of information security programs. The effectiveness and efficiency metrics require fusing security program activities data with the data obtained from monitoring and evaluation tools in a manner that can be directly tied to security controls implementation.

Impact metrics are used to articulate the impact of information security on the organization's mission, often through quantifying the cost savings produced by the security program or through costs incurred from addressing security events. These metrics combine information about the results of security controls implementation with a variety of information about resources. These metrics can provide the most direct insight into the value of security to the organization and are the ones that are sought out by executives. The impact metrics require tracking of a variety of resource information across the organization in a manner that can be directly tied to security activities and events.

Manageability is critical to the success of a metrics program. Organizations should limit the number of metrics collected to between five and ten metrics per stakeholder at a single time. Limiting this number will assist the organization in focusing efforts on correcting identified gaps.

5.2 Approach

The performance metrics development approach presented in this section describes how to develop implementation, efficiency/effectiveness, and impact metrics for information security and provides examples of these metrics. The approach explicitly connects information security activities to the organization's strategic goals through development and use of performance metrics. The approach assumes that organizations have multiple strategic goals and that a single goal may require inputs from metrics based on multiple security control families.

The performance metrics development approach provides two ways of developing metrics:

1. The control-specific approach selects individual controls as the basis for a metric that best represents the entire family as determined by the organizational environment.
2. The cross-cutting approach focuses on metrics that gauge security performance based on more than one individual control or control families. Multiple controls or control families are used in the development, collection, and analysis of the metric.

While both approaches will result in metrics that are representative in assessing where a given organization stands in support of the corresponding strategic objective, the cross-cutting metrics will provide a broader view of information security performance than the control-specific approach.

In the *control-specific* approach, the selected control and derived metric will:

- Be mapped directly to an individual control within the respective control family;
- Use the data describing the individual control's implementation to generate required metrics such as POA&M, testing, and project tracking; and

- Characterize the metric as applicable to low, moderate, or high system categorization.

In the *cross-cutting* approach the metric will:

- Be mapped to information security goals and objectives that may encompass performance of several information security controls belonging to several control families; and
- Use the data, describing the security program performance, to generate required metrics.

5.3 Metrics Development Template

Organizations should document their performance metrics in a standard format to ensure repeatability of metrics development, tailoring, collection, and reporting processes. A standard format will provide detail to guide metrics collection, analysis, and reporting activities. The candidate metric template, provided in this guide, is an example of such a template. Organizations may use a subset of the provided fields or may add more fields to the template based on their environment and requirements.

Table 2 lists the candidate metric template fields for both control-specific and cross-cutting approaches and highlights similarities and differences between the two templates. The table has four columns:

- Field—the name of the field in the template
- Purpose—the purpose of the field as it relates to metrics development
- Control-Specific Approach—specific guidance on filling out the field while following the control-specific approach
- Cross-Cutting Approach—specific guidance on filling out the field while following the cross-cutting approach.

Table 2. Metrics Development Template Description

Field	Purpose	Control-Specific Approach	Cross-Cutting Approach
Control Family or Control Families	NIST SP 800-53 control family or families that the metric addresses	Associated control family	Control families associated with the metric
Metric ID	Unique identifier for database and sorting purposes	Associated control number from NIST SP 800-53	Unique identifier assigned to the metric, to be determined by organization
Strategic Goal or Objective	Agency strategic goal or objective that the metric supports		
Information Security Goal	Statement of requirement or security goal for the candidate metric	Control family name and the corresponding FIPS 200 minimum security requirement specification.	Statement of security program goal related to applicable agency goal or objective

Field	Purpose	Control-Specific Approach	Cross-Cutting Approach
Control	Statement of individual control being measured	Description of NIST SP 800-53 control selected to represent the control family. When selecting such control, the organization should select the control that is most representative in assessing where the organization stands in the support of the corresponding strategic objective.	N/A
Control Enhancement	Control enhancement, if any, associated with the selected control	Description of NIST SP 800-53 control enhancement(s) for the selected control	N/A
Control Question	Control question that describes what this metric is measuring	Directly maps to the control or control enhancement that the metric is measuring	Identifies information required to measure accomplishment of security objective in a question format
Metric	Statement of measurement		
Metric Type	Statement of whether the metric is implementation, efficiency/effectiveness, or impact		
Frequency of data collection	Indication of how often the data is collected and analyzed to be reported internally or externally. In measuring organizational performance, trends are often more useful than individual snapshots. Frequent measurements provide data points for determining if the organization processes are improving or declining. Frequency will be determined by the stakeholder who expresses information need or through internal or external reporting requirements and will provide a cumulative measure over a period of time (statistics over a time span) or a snapshot. Frequency may also depend on a rate of change in a particular control that is being assessed. For example, any metrics that use incident statistics will have a higher frequency than budget-related metrics.		
Target	Minimum standard for a satisfactory rating for the metric. It can be an event such as milestone completion or a statistical measure. Targets can be expressed in percentages, time, dollars, or other appropriate units of measure. Targets can be temporal, in other words, a target may be tied to a required completion time frame. Interim targets are highly encouraged to enable tracking of progress toward stated objectives.		
Formula	Formula for calculating the metric		
Information Source	The organization(s) or function(s) responsible for collecting the metric data		
Related Control Families	To indicate dependencies for the metric with other control families	Listing of other NIST SP 800-53 control families that may affect, or be affected by, this metric.	N/A
Applicability (Low, Moderate, High)	To indicate corresponding security categorization for measured controls and focus data collection to applicable systems.	Security categorization as it applies to the individual control or control enhancement, addressed by the candidate metric.	N/A

Control-specific and cross-cutting metrics development templates are provided in Table 3 and Table 4.

Table 3. Control-Specific Metrics Development Approach Template

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family				
Metric ID				
Strategic Goal or Objective				
Information Security Goal	*Specification for minimum security requirements as stated in FIPS 200, Section 3.*			
Control				
Control Enhancement(s)	NOTE: Shade this row if control enhancements do not apply.			
Control Question(s)				
Metric(s)				
Metric Type(s)				
Frequency(ies)				
Target(s)				
Formula(s)				
Information Source				
Related Control Families				

Table 4. Cross-Cutting Metrics Development Approach Template

Cross-Cutting Approach Template	
	Details
Control Families	
Metric ID	
Strategic Goal or Objective	
Information Security Goal	
Control Question(s)	
Metric(s)	
Metric Type(s)	
Frequency(ies)	
Target(s)	
Formula(s)	
Information Source	

5.4 Candidate Metrics

Devoting sufficient time to establishing information security performance metrics is critical to deriving the maximum value from measuring information security performance.

The impact of devoting sufficient time to setting up the program in advance is similar to that of devoting sufficient time to requirements definition in system development—investing time early in the process is more effective than retrofitting requirements when the effort is under way. Each organization will undertake a number of activities to set up a security performance metrics program to include:

- Selecting the metrics that are most appropriate for the organization's strategy and business environment, including mission and security priorities, environment, and requirements;
- Taking time to collect input from, get buy-in, and educate all relevant stakeholders; and

- Ensuring that appropriate technical and process infrastructure is in place, including modification or creation of data collection, analysis, and reporting tools.

NIST SP 800-55 identifies a process for setting up an information security metrics program.

This section offers 18 candidate metrics: one for each security control family in NIST SP 800-53 and one overall policy metric. These metrics are examples that organizations can adopt to measure performance of their information security programs. Organizations should look into developing other metrics if the metrics provided in this section are not appropriate for their needs. The candidate metrics provide examples of control-specific and cross-cutting approaches and include all metrics types—implementation, effectiveness/efficiency, and impact. Tables 5 through 22 list the candidate metrics. All quotes from FIPS 200 and NIST SP 800-53 are italicized.

Table 5. Access Control (AC) Cross-Cutting Approach

Cross-Cutting Approach Template	
	Details
Control Families	Access Control, Incident Response, Configuration Management
Metric ID	Unique identifier to be filled out by the organization
Strategic Goal or Objective	Enhance the use of information technology in service delivery and record keeping.
Information Security Goal	Restrict information, system, and component access to individuals or machines that are identifiable, known, credible, and authorized.
Control Question(s)	Are access control security controls effectively preventing security incidents?
Metric(s)	Percentage (%) of security incidents caused by improperly configured access controls
Metric Type(s)	Effectiveness
Frequency(ies)	Organization-defined (example: quarterly)
Target(s)	Organization-defined (example: 10%)
Formula(s)	(# of incidents related to access control / total # of incidents) *100
Information Source	Chief Information Officer (CIO), Computer Security Incident Response Team (CSIRT), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Administrator

Table 6. Awareness and Training (AT) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Awareness and Training			
Metric ID	AT-4 Security Training Records	X	X	X
Strategic Goal or Objective	To modernize the organization through its people, processes, and technology.			
Information Security Goal	*Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.*			
Control	*The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.*	X	X	X
Control Enhancement(s)				
Control Question(s)	Do records indicate that system users are provided awareness training?	X	X	X
	Do records indicate that information system security personnel are continually trained in their duties?	X	X	X
Metric(s)	Percentage (%) of system users that have received basic awareness training	X	X	X
	Percentage (%) of information system security personnel that have received security training[12]	X	X	X
Metric Type(s)	Implementation	X	X	X
	Implementation	X	X	X
Frequency(ies)	Organization-defined (example: at least annually)	X	X	X
	Organization-defined (example: at least annually)	X	X	X
Target(s)	Organization-defined (example: 100%)	X	X	X
	Organization-defined (example: 100%)	X	X	X
Formula(s)	(# of system users that have completed awareness training, according to records / total # of system users) * 100	X	X	X
	(# of information system security personnel that have completed security training within the past year / total # of information system security personnel) * 100	X	X	X
Information Source	Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), Training Manager			
Related Control Families	None			

[12] Similar metrics can be found in NIST SP 800-55.

Table 7. Audit and Accountability (AU) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Audit and Accountability			
Metric ID	AU-6 Audit Monitoring, Analysis, and Reporting		X	X
Strategic Goal or Objective	Enhance the use of information technology in service delivery and record keeping.			
Information Security Goal	*Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.*			
Control	*The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.*		X	X
Control Enhancement(s)	*(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.*			X
	(2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.			
Control Question(s)	How often does the organization analyze audit records for violations?		X	X
	Does the organization report findings to officials for further investigation?		X	X
	Are automated mechanisms used in the analysis and reporting process?			X
Metric(s)	Average frequency of audit records review and analyses for inappropriate activity		X	X
	Percentage of audit log findings reported to appropriate officials		X	X
	Percentage of systems using automated mechanisms to conduct analysis and reporting of inappropriate activities			X
Metric Type(s)	Efficiency		X	X
	Implementation		X	X
	Implementation			X
Frequency(ies)	Organization-defined (example: quarterly assessment)		X	X
	Organization-defined (example: quarterly assessment)		X	X
	Organization-defined (example: annual assessment)			X
Target(s)	Organization-defined (example: daily)		X	X
	Organization-defined (example: 90%)		X	X
	Organization-defined (example: 90%)			X
Formula(s)	Average frequency during reporting period		X	X
	(# of findings reported to appropriate officials / total # of findings) * 100		X	X
	(# of systems with automated mechanisms in process / total # of systems) * 100			X
Information Source	Chief Information Officer (CIO), Computer Security Incident Response Team (CSIRT), Human Resources, Information System Security Officer (ISSO), Office of the Inspector General, Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Owner			
Related Control Families	Access Control, Identification and Authentication, Incident Response, Physical and Environmental Protection, Personnel Security, Risk Assessment			

Table 8. Certification, Accreditation, and Security Assessments (CA) Cross-Cutting Approach

Cross-Cutting Approach Template	
	Details
Control Families	Certification, Accreditation, and Security Assessments
Metric ID	Unique identifier to be filled out by the organization
Strategic Goal or Objective	Achieve excellence in management practices.
Information Security Goal	*Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.*
Control Question(s)	How effective is the organization's C&A process?
Metric(s)	Percentage (%) of operational systems that have completed C&A following major changes
	Percentage (%) of new systems that completed C&A prior to the implementation
Metric Type(s)	Effectiveness
	Effectiveness
Frequency(ies)	Organization-defined (example: annually)
	Organization-defined (example: annually)
Target(s)	Organization-defined (example: 100%)
	Organization-defined (example: 100%)
Formula(s)	(# of operational systems with complete C&A updates following major changes / total # of operational systems with major changes) * 100
	(# of new systems with complete C&A packages prior to implementation / total # of new systems) * 100
Information Source	Certifying Authority (CA), Chief Information Officer (CIO), Designated Approving Authority (DAA), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])

Table 9. Configuration Management (CM) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Configuration Management			
Metric ID	CM-2 Baseline Configuration and System Component Inventory		X	X
Strategic Goal or Objective	Manage information technology resources to improve service for our customers and partners.			
Information Security Goal	*Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.*			
Control	*The organization develops, documents, and maintains a current baseline configuration of the information system, an inventory of the system's constituent components, and relevant ownership information.*	X	X	X
Control Enhancement(s)	*(1) The organization updates the baseline configuration of the information system and inventory of system components as an integral part of information system component installations.*		X	X
	(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system and inventory of information system components.			X
Control Question(s)	Does the organization follow established processes to manage system configuration changes?	X	X	X
	Does the organization update the baseline configuration to include each approved configuration change?		X	X
Metric(s)	Percentage (%) of systems that are compliant with the baseline configuration	X	X	X
	Percentage (%) of configuration changes documented in the latest baseline configuration		X	X
Metric Type(s)	Implementation	X	X	X
	Implementation		X	X
Frequency(ies)	Organization-defined (example: at least annually)	X	X	X
	Organization-defined (example: at least annually)		X	X
Target(s)	Organization-defined (example: 100% of high, 90% of moderate, 80% of low)	X	X	X
	Organization-defined (example: 90% of high)		X	X
Formula(s)	(# of systems that comply with the approved baseline / total # of systems in inventory) * 100	X	X	X
	(# of documented baseline system configuration changes/ total # of configuration changes identified through automated scans) * 100		X	X
Information Source	Configuration Control Board, Information System Security Officer (ISSO), System Administrator, System Owner			
Related Control Families	Certification, Accreditation, and Security Assessments			

Table 10. Contingency Planning (CP) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Contingency Planning			
Metric ID	CP-4 Contingency Plan Testing		X	X
Strategic Goal or Objective	Identify and assess the vulnerability of critical infrastructure and key assets.			
Information Security Goal	*Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.*			
Control	*The organization tests the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.*		X	X
Control Enhancement(s)	*(1) The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).*		X	X
	(2) The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.			X
	(3) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.			
Control Question(s)	What method(s) is (are) selected for testing the contingency plan? How often is the contingency plan tested?		X	X
	What organizational elements have participated in the testing of the contingency plan? Were the results of the test documented?		X	X
	Did the contingency plan get tested at the alternate processing site?			X
Metric(s)	Percentage (%) of systems successfully addressed in the testing of the contingency plan		X	X
	Percentage (%) of systems successfully coordinating contingency plan testing with testing of other plans, such as Incident Response Plan, Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan		X	X
	Percentage (%) of systems successfully testing the contingency plan at the alternate processing site			X
Metric Type(s)	Effectiveness		X	X
	Implementation		X	X
	Implementation			X
Frequency(ies)	Organization-defined (example: at least annually)		X	X
	Organization-defined (example: at least annually)		X	X
	Organization-defined (example: at least annually)			X
Target(s)	Organization-defined (example: 100% of high, 90% of moderate)		X	X
	Organization-defined (example: 100% of high, 90% of moderate)		X	X
	Organization-defined (example: 90% of high)			X
Formula(s)	(# of systems that successfully participated in the contingency plan testing, including developing lessons-learned and documenting in the POA&M / # of systems in inventory) * 100		X	X
	(# of systems successfully coordinating CP testing with testing of other plans / total # of systems in inventory) * 100		X	X
	(# of systems successfully testing the CP at the alternate processing site / total # of systems) * 100			X
Information Source	Chief Information Officer (CIO), Computer Security Incident Response Team (CSIRT), Senior Agency Information Security Officer (SAISO) (e.g., CISO), Contingency Planning Manager, Physical Security Officer			
Related Control Families	Incident Response (IR)			

Table 11. Identification and Authentication (IA) Control-Specific Approach

Cross-Cutting Approach Template	
	Details
Control Families	Identification and Authentication, Access Control, Configuration Management
Metric ID	Unique identifier to be filled out by the organization
Strategic Goal or Objective	Enhance the use of information technology in service delivery and record keeping.
Information Security Goal	All users accessing the organization's systems are uniquely identified and authenticated.
Control Question(s)	Have individuals that are not uniquely identifiable, known, credible, and authorized been allowed access to organizational systems, components, or information?
Metric(s)	Percentage of accounts not associated with specific users
Metric Type(s)	Effectiveness
Frequency(ies)	Organization-defined (example: monthly)
Target(s)	Organization-defined (example: zero)
Formula(s)	(# of group, default, guest, blank, and other non-specific user accounts / total # of accounts) * 100
Information Source	Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Administrator

Table 12. Incident Response (IR) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Incident Response			
Metric ID	IR-6 Incident Reporting	X	X	X
Strategic Goal or Objective	Promote the integrity of information systems.			
Information Security Goal	*Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.*			
Control	*The organization promptly reports incident information to appropriate authorities.*	X	X	X
Control Enhancement(s)	*(1) The organization employs automated mechanisms to assist in the reporting of security incidents.*		X	X
Control Question(s)	Does the organization and its subordinate organizations report incident information to appropriate authorities, such as the Department of Homeland Security United States Computer Emergency Readiness Team (DHS US-CERT) and the Intelligence Community-Incident Response Center (IC-IRC), in accordance with federal reporting requirements and timelines for Sensitive But Unclassified (SBU) and IC systems, respectively? Are the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations consistent with applicable federal laws, directives, policies, regulations, standards, and guidance?	X	X	X
	Has the organization employed automated mechanisms, such as web-based reporting or secure electronic data transfer, to assist in the reporting of security incidents?		X	X
Metric(s)	Percentage (%) of SBU incidents for all systems reported to US-CERT Percentage (%) of IC incidents reported to IC-IRC	X	X	X
	Percentage (%) of systems employing automated mechanisms, such as web-based reporting or secure electronic data transfer, to assist in the reporting of security incidents		X	X
Metric Type(s)	Implementation	X	X	X
	Implementation		X	X
Frequency(ies)	Organization-defined (example: monthly)	X	X	X
	Organization-defined (example: annually)		X	X
Target(s)	Organization/US-CERT-defined (example: 100%) Organization/IC-IRC-defined (example: 90%)	X	X	X
	Organization-defined (example: 90%)		X	X
Formula(s)	(# of SBU incidents reported to US-CERT / total # of SBU incidents) * 100 (# of IC incidents reported to IC-IRC / total # of IC incidents) * 100	X	X	X
	(# of systems employing automated mechanisms in IR reporting / total # of systems) * 100		X	X
Information Source	Chief Information Officer (CIO), Computer Security Incident Response Team (CSIRT), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Owner			
Related Control Families	None			

Table 13. Maintenance (MA) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Maintenance			
Metric ID	MA-2 Periodic Maintenance	X	X	X
Strategic Goal or Objective	Achieve excellence in management practices.			
Information Security Goal	*Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.*			
Control	*The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.*	X	X	X
Control Enhancement(s)	*(1) The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).*		X	X
	(2) The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.			X
Control Question(s)	Does the organization perform information system component maintenance according to required schedule?	X	X	X
	Does the organization use automated tools to ensure that periodic maintenance is performed on systems, as required?			X
Metric(s)	Percentage (%) of system components that undergo maintenance on schedule	X	X	X
	Percentage (%) of systems that use automated tools to validate performance of periodic maintenance			X
Metric Type(s)	Efficiency	X	X	X
	Implementation			X
Frequency(ies)	Organization-defined (example: quarterly)	X	X	X
	Organization-defined (example: annually)			X
Target(s)	Organization-defined (example: 90%)	X	X	X
	Organization-defined (example: 90%)			X
Formula(s)	(# of system components that underwent scheduled maintenance / total # of system components scheduled for maintenance) * 100	X	X	X
	(# of systems that use automated tools / total # of systems) * 100			X
Information Source	Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Administrator			
Related Control Families	None			

Table 14. Media Protection (MP) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Media Protection			
Metric ID	MP-6 Media Sanitization and Disposal	X	X	X
Strategic Goal or Objective	Enhance the use of information technology in service delivery and record keeping.			
Information Security Goal	*Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.*			
Control	*The organization: (i) sanitizes information system media, both paper and digital, prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii) periodically tests sanitization equipment and procedures to ensure correct performance.*	X	X	X
Control Enhancement(s)				
Control Question(s)	Does the organization have a process for sanitizing digital media?	X	X	X
	How effective is the organization's process for sanitizing digital media?	X	X	X
Metric(s)	Percentage of media that passes sanitization procedures testing	X	X	X
Metric Types(s)	Effectiveness	X	X	X
Frequency(ies)	Quarterly	X	X	X
Target(s)	Organization-defined	X	X	X
Formula(s)	(# of media that passes sanitization procedures testing / total # of media tested) * 100	X	X	X
Information Source	Information System Security Officer (ISSO)			
Related Control Families	None			

Table 15. Physical and Environmental Protection (PE) Cross-Cutting Approach

Cross-Cutting Approach Template	
	Details
Control Family	Physical and Environmental Protection, Access Control, Incident Response
Metric ID	Unique identifier to be filled out by the organization
Strategic Goal or Objective	Manage information technology resources, using e-gov, to improve service for our customers and partners.
Information Security Goal	Integrate physical and information security protection mechanisms to ensure appropriate protection of organization's information resources.
Control Question(s)	Has the organization implemented appropriate physical security measures to reduce the risks to its information resources?
Metric(s)	Percentage of physical security incidents allowing unauthorized entry into facility containing information systems
	Percentage of information security incidents caused by physical access control failures
	Cost of information security incidents of unauthorized access to information systems, due to physical security failures[13]
Metric Type(s)	Effectiveness
	Effectiveness
	Impact
Frequency(ies)	Organization-defined (example: monthly report)
	Organization-defined (example: quarterly report)
	Organization-defined (example: quarterly report)
Target(s)	Organization-defined (example: zero)
	Organization-defined
	Organization-defined
Formula(s)	(# of physical security incidents allowing unauthorized entry / total # of physical security incidents) * 100
	(# of information security incidents due to physical security breach / total # of information security incidents) * 100
	sum of costs of each incident within the reporting period
Information Source	Computer Security Incident Response Team (CSIRT), Physical Security Office

[13] Similar impact metrics, cross-cutting or control-specific, can be created using other controls.

Table 16. Planning (PL) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Planning			
Metric ID	PL-4 Rules of Behavior[14]	X	X	X
Strategic Goal or Objective	To modernize the organization through its people, processes, and technology.			
Information Security Goal	*Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.*			
Control	*The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.*	X	X	X
Control Enhancement				
Control Question(s)	Has the organization established a process for ensuring that all users have signed an acknowledgement that they have read, understood, and agree to abide by the rules of behavior, before they are authorized access to the information system?	X	X	X
Metric(s)	Percentage (%) of employees who signed acknowledgement that they have read and understood rules of behavior, before being authorized access to the information system	X	X	X
Metric Type(s)	Implementation	X	X	X
Frequency(ies)	Organization-defined (example: annually)	X	X	X
Target(s)	Organization-defined (example: 100%)	X	X	X
Formula(s)	(# of users who signed rules of behavior / total # of users with system access) * 100	X	X	X
Information Source	Chief Information Officer (CIO), Human Resources, Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Owner			
Related Control Families	Certification, Accreditation, and Security Assessments			

[14] For a metric on System Security Plans, see NIST SP 800-55.

Table 17. Personnel Security (PS) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Personnel Security			
Metric ID	PS-3 Personnel Screening	X	X	X
Strategic Goal or Objective	Protect confidentiality and data integrity to ensure privacy and security.			
Information Security Goal	*Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.*			
Control	*The organization screens individuals requiring access to organizational information and information systems before authorizing access.*	X	X	X
Control Enhancement				
Control Question(s)	Does the organization appropriately screen individuals requiring access to organizational information and information systems before authorizing access?	X	X	X
Metric(s)	Percentage (%) of individuals screened before being granted access to organizational information and information systems	X	X	X
Metric Type(s)	Implementation	X	X	X
Frequency(ies)	Organization-defined (example: at least annually)	X	X	X
Target(s)	Organization-defined (example: 100%)	X	X	X
Formula(s)	(# of individuals screened / total # individuals with access) * 100	X	X	X
Information Source	Facility Security Officer, Information System Security Officers (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Owner			
Related Control Families	Access Control, Identification and Authentication, Physical and Environmental Protection, Planning			

Table 18. Risk Assessment (RA) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	Risk Assessment			
Metric ID	RA-5 Vulnerability Scanning[15]		X	X
Strategic Goal or Objective	Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to the organization's stakeholders.			
Information Security Goal	*Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.*			
Control	*The organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities affecting the system are identified and reported.*		X	X
Control Enhancement(s)	*(1) Vulnerability scanning tools include the capability to readily update the list of information system vulnerabilities scanned.*			X
	(2) The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when significant new vulnerabilities are identified and reported.			X
	(3) Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.			
Control Question(s)	How efficiently does the organization remediate high-risk vulnerabilities identified during vulnerability scans?		X	X
	Does vulnerability scanning help prevent incidents on the organization's systems and networks?		X	X
Metric(s)	Percentage (%) of high-risk vulnerabilities remediated within organization-specified timeframe		X	X
	Percentage (%) of incidents caused by known vulnerabilities		X	X
Metric Type(s)	Efficiency		X	X
	Effectiveness		X	X
Frequency(ies)	Organization-defined (example: monthly)		X	X
	Organization-defined (example: monthly)		X	X
Target(s)	Organization-defined (example: 80%)		X	X
	Organization-defined (example: 10%)		X	X
Formula(s)	(# of high-risk vulnerabilities remediated within organization-defined period (e.g., 30 days) / total # of high-risk vulnerabilities identified in vulnerability scans) * 100		X	X
	(# of incidents caused by vulnerabilities that were identified through scanning but not remediated / total # of incidents) * 100		X	X
Information Source	Chief Information Officer (CIO), Computer Security Incident Response Team (CSIRT), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Administrator, System Owner, Vulnerability Assessment Team			
Related Control Families	Incident Response (IR)			

[15] Risk assessment metrics are available in NIST SP 800-55.

Table 19. System and Services Acquisition (SA) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	System and Services Acquisition			
Metric ID	SA-4 Acquisitions	X	X	X
Strategic Goal or Objective	Enhance the efficiency and effectiveness of competitive sourcing			
Information Security Goal	*Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.*			
Control	*The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.*	X	X	X
Control Enhancement(s)				
Control Question(s)	Are security requirements included in new systems and service acquisitions?	X	X	X
	Has the organization put in place a process to monitor compliance with security requirements by their system and service providers?	X	X	X
Metric(s)	Percentage (%) of system and service acquisition contracts that include security requirements and/or specifications	X	X	X
	Percentage (%) of system and service acquisition contracts that require regular reporting of compliance with security requirements	X	X	X
	Percentage (%) of contractors that are fully compliant with security requirements, identified in applicable system and services acquisition contracts	X	X	X
Metric Type(s)	Implementation	X	X	X
	Implementation	X	X	X
	Effectiveness	X	X	X
Frequency(ies)	Organization-defined (example: annually)	X	X	X
	Organization-defined (example: annually)	X	X	X
	Organization-defined (example: at least annually)	X	X	X
Target(s)	Organization-defined (example: 100%)	X	X	X
	Organization-defined (example: 100%)	X	X	X
	Organization-defined (example: 100%)	X	X	X
Formula(s)	(# of system and service acquisition contracts that include security requirements and/or specifications / total # of system and service acquisition contracts) * 100	X	X	X
	(# of system and service acquisition contracts that require regular compliance reporting / total # of system and service acquisition contracts) * 100	X	X	X
	(# of compliant contractors / total # of contracts) * 100	X	X	X
Information Source	Contracting Officer, Contracting Officer's Technical Representative, Procurement Officers, Information System Security Officers (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Owner			
Related Control Families	Certification, Accreditation, and Security Assessments, Configuration Management, Planning, Risk Assessment			

Table 20. System and Communications Protection (SC) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	System and Communications Protection			
Metric ID	SC-7 Boundary Protection	X	X	X
Strategic Goal or Objective	Protect confidentiality and data integrity to ensure privacy and security.			
Information Security Goal	*Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.*			
Control	*The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.*	X	X	X
Control Enhancement(s)	*(1) The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.*		X	X
Control Question(s)	Are all external boundaries protected and monitored for inappropriate activity?	X	X	X
	Did a failure in boundary protection mechanisms cost the organization in information security incidents?		X	X
Metric(s)	Percentage (%) of external communications systems which use controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels)	X	X	X
	Cost of information security incidents [resulting in unauthorized release of information outside the information system boundary] due to operational failure of boundary protection mechanisms[16]		X	X
Metric Type(s)	Implementation	X	X	X
	Impact		X	X
Frequency(ies)	Organization-defined (example: monthly)	X	X	X
	Organization-defined (example: quarterly)		X	X
Target(s)	Organization-defined (example: 100%)	X	X	X
	Organization-defined		X	X
Formula(s)	(# of external systems protected by controlled interfaces / total # of external systems) * 100	X	X	X
	Sum of costs resulting from incidents caused by failure, based on remediation resources, loss in direct productivity, and other related costs		X	X
Information Source	Chief Information Officer (CIO), Computer Security Incident Response Team (CSIRT), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Security Officer, System Owner			
Related Control Families	Configuration Management, Incident Response, Maintenance, Risk Assessment			

[16] This metric can be used as a model for other impact metrics.

Table 21. System and Information Integrity (SI) Control-Specific Approach

Control-Specific Approach Template				
		Applicability		
	Details	L	M	H
Control Family	System and Information Integrity			
Metric ID	SI-5 Security Alerts and Advisories	X	X	X
Strategic Goal or Objective	Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to partners and the public.			
Information Security Goal	*Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.*			
Control	*The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.*	X	X	X
Control Enhancement(s)	*(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.*			
Control Question(s)	Are applicable alerts disseminated throughout the organization?	X	X	X
	Are remediation actions taken to address known vulnerabilities?	X	X	X
Metric(s)	Percentage (%) of applicable alerts and advisories disseminated throughout the organization	X	X	X
	Percentage (%) of applicable weaknesses for which the patches have been applied or that have been otherwise mitigated	X	X	X
Metric Type(s)	Implementation	X	X	X
	Effectiveness	X	X	X
Frequency(ies)	Organization-defined (example: monthly)	X	X	X
	Organization-defined (example: monthly)	X	X	X
Target(s)	Organization-defined (example: 100%)	X	X	X
	Organization-defined (example: 90%)	X	X	X
Formula(s)	(# of alerts/advisories issued by the organization/ total # of applicable US-CERT alerts/advisories) *100	X	X	X
	(# of systems reporting patch is NA, implemented, or waiver granted / total # of systems in inventory) * 100	X	X	X
Information Source	Chief Information Officer (CIO), Computer Security Incident Response Team (CSIRT), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Administrator, System Owner			
Related Control Families	Configuration Management, Incident Response			

Table 22. Overall Metrics Policy Cross-Cutting Approach

Cross-Cutting Approach Template	
	Details
Control Family	All
Metric ID	Unique identifier to be filled out by the organization
Strategic Goal or Objective	Achieve excellence in management practices.
Information Security Goal	*The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented policy for each applicable security control that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the policies and associated controls.*
Control Question(s)	Has the organization developed policies and corresponding procedures to cover all NIST SP 800-53 control families?
	Does the organization have a mechanism to ensure that policies and procedures are communicated to its employees?
Metric(s)	Percentage (%) of NIST SP 800-53 control families for which policies and procedures exist
	Percentage (%) of employees who signed acknowledgement that they have read and understood policies and procedures
Metric Types(s)	Implementation
	Implementation
Frequency(ies)	Organization-defined (example: annually)
	Organization-defined (example: bi-annually)
Target(s)	Organization-defined (example: 100%)
	Organization-defined (example: 100%)
Formula(s)	(# of control families for which policies and procedures exist / 17) * 100
	(# of employees who signed acknowledgement/total number of employees) * 100
Information Source	Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer (CISO), System Owner

6. Conclusion

Tracking and measuring program performance is critical to any program's ability to achieve success. Measurement assists with pinpointing problems, scoping the resources for remediation, tracking status of remediation, and quantifying successes. Measurement also creates accountability for results by tracking ownership of data and completion of activities associated with the data. Finally, measurement is essential to performance improvement, because it quantifies performance gaps and provides insights into root causes of inadequate performance. Federal agencies are required to collect and report performance measures to comply with GPRA and FISMA, and in response to the PMA initiative. Organizations may also be collecting and reporting organization-specific performance measures for internal management purposes. Information security performance metrics support existing requirements and assist in internal efforts to improve information security.

This guide describes an approach for linking information security performance to agency-level strategic planning and mission execution, through the development of information security performance measures that are mapped to agency-level strategic goals and objectives. The guide uses NIST SP 800-53 security controls to characterize security performance and provides at least one candidate metric for each of the 17 control families. The templates and candidate metrics contained in this guide are offered as sample tools to information security practitioners and are meant to facilitate implementation and use of information security performance metrics. Security practitioners are encouraged to use this guide to develop additional metrics to demonstrate how information security programs support their organizations' missions.

Appendix A: Acronyms

CSIRT	Computer Security Incident Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
GPRA	Government Performance Results Act of 1993
IC-IRC	Intelligence Community-Incident Response Center
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PMA	President's Management Agenda
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Officer
SBU	Secret But Unclassified
SP	Special Publication
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team

Appendix B: References

Public Law 103-62, Government Performance and Results Act of 1993.

Public Law 104-106, Clinger-Cohen Act, 1996.

Federal Information Management Security Act (Public Law 107-347) of 2002.

Office of Management and Budget Circular A-11, *Preparation, Submission, and Execution of the Budget*, Part 6, 2005.

Office of Management and Budget Circular A-130. Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Systems*, March 2006.

National Institute of Standards and Technology Special Publication 800-53, Public Draft, Revision 1, *Recommended Security Controls for Federal Information Systems*, March 2006.

National Institute of Standards and Technology Special Publication 800-53A, Second Public Draft, *Guide for Assessing the Security Controls in Federal Information Systems*, April 2006.

National Institute of Standards and Technology Special Publication 800-55, *Security Metrics for Information Technology Systems*, July 2003.

National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

National Institute of Standards and Technology Special Publication 800-100, *Draft Information Security Handbook: A Guide for Managers*, 2006.