NIST
“Security Metrics Guide for Information Technology Systems”

July 2003

Purpose of this document

"provides guidance on how an organization, through the **use of metrics, identifies the adequacy of in-place security** controls, policies, and procedures."

- "It provides an approach to **help management decide where to invest** in additional security protection resources or identify and evaluate nonproductive controls."
- "It **explains the metric development and implementation** process and how it can also be used to adequately **justify security control investments**."

Comparison of NIST & PSM Guidelines

Measurement Objective

NIST

A metric program will produce “useful data for directing the **allocation of information security resources** and should simplify the preparation of performance-related [**OMB Performance Measurement**] reports.”

PSM

Objective data to support various **management decisions**

Comparison (2)

Organizational Level

NIST

This document defines a measurement process that is applicable from the **“Head of the Agency” to the “Program Manager/System Owner.”** This document is also targeted for **Government** organizations.

PSM

Focus is on any **Project Manager**

Comparison (3)

Implementing a Measurement Process

NIST

"The establishment of a metrics program will require a **substantial investment** to ensure that the program is properly implemented to **maximize its benefits**."

PSM

Start small, use existing data.

Information Needs of the NIST document

"Benefits of a security metrics program"

- **accountability** for security
- **pinpoint specific problems** in technical, operational, or management controls justify investment requests,
- justify **investment** requests,
- demonstrate **compliance** with applicable laws, rules, and regulations
- **Meets OMB reporting** requirement for performance measures, plus GAO and IG audits

NIST Categories of Measures

"Organizations can develop and collect metrics of three types:

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

"The type of metric depends on where the system is within its life cycle and the maturity of the IT system security program."

Overview of the NIST Measurement Process [Section 4 of the document]

METRICS DEVELOPMENT AND IMPLEMENTATION APPROACH

- 4.1 Metrics Development Process
  - 4.1.1 Stakeholder Interest Identification
  - 4.1.2 Goals and Objectives Definition
  - 4.1.3 IT Security Policies, Guidance, and Procedures Review
  - 4.1.4 System Security Program Implementation Review
  - 4.1.5 Metrics Development and Selection
- 4.2 Establishing Performance Targets
- 4.3 Feedback Within Metrics Development Process

NIST Equivalent of a Measurement Specification

- Go to Word

APPENDIX A: SAMPLE IT SECURITY METRICS

"Table A-1 [following] provides a quick reference guide for finding specific metrics that directly correspond to the 2003 OMB FISMA [Federal Information Security Management Act] guidance questions."

Critical Element	**Metric**	**OMB Guidance Reference**
[see the following table]		