NIST Security Measurement
NIST SP 800-55 Revision 1

Information Security and Privacy Advisory Board
September 6, 2007

Curt Barker
Chief, Computer Security Division (CSD)
Information Technology Laboratory (ITL)
NIST SP 800-55 Rev 1 Overview

- Describes approach for development and implementation of information security measurement program to
  - Develop, select, and implement information system-level and program-level measures
  - Guide an organization on how to identify the adequacy of in-place security controls, policies, and procedures through the use of measures

- Provides an approach to help management decide where to invest in additional information security resources, identify and evaluate nonproductive security controls, and prioritize security controls for continuous monitoring

- Explains use of measures to adequately justify information security investments and support risk-based decisions
Information Security Measurement Program Scope

- Information security measurement program scope can fit a variety of contexts
  - Quantifying information system-level security performance for an operational information system
  - Quantifying the integration of information security into the SDLC during information system and software development processes
  - Quantifying enterprise-wide information security performance

- Scope can encompass organizational units, sites, or other organizational constructs and be based on
  - Stakeholder needs
  - Strategic goals and objectives
  - Operating environments
  - Risk priorities
  - Information security program maturity
Information Security Measurement Program Structure

1. Foundation of upper-level management support is critical
2. Information Security Policies & Procedures must be backed by authority necessary to enforce compliance
3. Develop quantifiable performance measures to capture/provide meaningful performance data
4. Information security measurement program must emphasize consistent periodic analysis of the measures data
Benefits of Using Measures

• **Increase Accountability**
  - Help identify security controls that are implemented incorrectly, are not implemented, or are ineffective
  - Facilitate identification of the personnel responsible for security controls implementation

• **Improve Information Security Effectiveness**
  - Quantify improvements in securing information systems
  - Demonstrate quantifiable progress in accomplishing strategic goals and objectives
  - Determine the effectiveness of implemented information security processes, procedures, and security controls

• **Demonstrate Compliance**
  - Assist in satisfying the annual FISMA reporting requirements
  - Use as input into GAO and IG audits
  - Demonstrate agency commitment to proactive information security

• **Provide Quantifiable Inputs for Resource Allocation Decisions**
  - Contribute quantifiable information to the risk management process
  - Allow measurement of successes and failures of past and current information security investments
  - Provide a solid baseline for business case development
Relationship to Other NIST Documents

- **NIST SP 800-53A**
- **NIST SP 800-30**
- **NIST SP 800-53**

**NIST SP 800-55 Rev1**
- Quantitative approach to measuring and analyzing security implementation and effectiveness aggregated across multiple individual efforts
- Approach for aggregating information efforts to obtain enterprise-level perspective
- Inputs into the information security program activities
- Inputs into prioritization for the continuous monitoring and improvement
- Supersedes 800-55 and Draft 800-80

**Data Sources**
- NIST SP 800-100
- NIST SP 800-65
- NIST SP 800-37

**Inputs**
- 800-30, *Risk Management Guide for Information Technology Systems*
- 800-53, *Recommended Security Controls for Federal Information Systems*
- 800-65, *Integrating Security into the Capital Planning and Investment Control Process*
Types of Measures

• *Implementation* measures to track progress in implementing information security controls
  - Percentage of individuals screened before being granted access to organizational information and information systems
  - Percentage of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior % of trained personnel
  - Percentage of information system security personnel that have received security training

• *Effectiveness/efficiency* measures to track results of security control implementation
  - Percentage of vulnerabilities remediated within organization-specified timeframes
  - Percentage of physical security incidents allowing unauthorized entry into facilities containing information systems
  - Percentage of remote access points used to gain unauthorized access

• *Impact* measures to articulate the impact of information security on the organization’s mission
  - Cost of virus attacks
  - Cost of incident recovery
  - Cost of downtime
# Measures Template

<table>
<thead>
<tr>
<th>Measure ID</th>
<th>Unique identifier used for measure tracking and sorting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal and Objective</td>
<td>Statement of information security goal and objective, may include strategic goal</td>
</tr>
<tr>
<td>Measure</td>
<td>Statement of measurement-use a numeric statement beginning with “percentage”, “number”, “frequency”, “average”, or similar term</td>
</tr>
<tr>
<td>Measure Type</td>
<td>Whether the measure is implementation, effectiveness/efficiency, or impact</td>
</tr>
<tr>
<td>Formula</td>
<td>Calculation to be performed that results in a numeric expression of a metric</td>
</tr>
<tr>
<td>Target</td>
<td>Threshold for a satisfactory rating for the measure, expressed in %, time, $, etc.</td>
</tr>
<tr>
<td>Implementation Evidence</td>
<td>Specific questions that will need to be answered via survey or through automatic data gathering to be able to calculate the metric</td>
</tr>
<tr>
<td>Frequency</td>
<td>How often the date is collected/analyzed, and how often the data is reported</td>
</tr>
<tr>
<td>Responsible Parties</td>
<td>Indicate the following key stakeholders: Information Owner, Information Collector, and Information Customer</td>
</tr>
<tr>
<td>Data Source</td>
<td>Lists the location of the data to be used in calculating the measure</td>
</tr>
<tr>
<td>Reporting Format</td>
<td>Indication of how the measure will be reported, e.g. pie chart, line chart, bar graph</td>
</tr>
</tbody>
</table>
# Example – System and Service Acquisition

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure ID</td>
<td>Service Acquisition Contract Measure 1 (or a unique identifier to be filled out by the organization)</td>
</tr>
</tbody>
</table>
| Goal and Objective     | • *Strategic Goal:* Accelerate the development and use of an electronic information infrastructure  
                          • *Information Security Goal:* Ensure third party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization                                      |
| Measure                | Percentage (%) of system and service acquisition contracts that include security requirements and/or specifications  
                          NIST SP 800-53 Control – SA-4: Acquisitions                                                                                                                                                                                                                       |
| Measure Type           | Implementation                                                                                                                                                                                                                                                              |
| Formula                | (Number of system and service acquisition contracts that include security requirements and specifications/total number of system and service acquisition contracts) * 100  
                          Target This should be a high percentage defined by the organization                                                                                                                                          |
| Implementation Evidence| 1. How many active service acquisition contracts does the organization have? _____  
                          2. How many active service acquisition contracts include security requirements and specifications (SA-4)? ________                                                                                                                                 |
| Frequency              | Collection Frequency: Organization-defined (example: quarterly)  
                          Reporting Frequency: Organization-defined (example: annually)                                                                                                                                                                                                                  |
| Responsible Parties    | • Information Owner: Organization-defined (example: Contracting Officer)  
                          • Information Collector: Organization-defined (example: Contracting Officer’s Technical Representative, System Owner)  
                          • Information Customer: Contracting Officer’s Technical Representative, System Owner, Procurement Officer, Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]) |
| Data Source            | Service acquisition contracts                                                                                                                                                                                                                                               |
| Reporting Format       | Pie chart comparing the percentage of system and service acquisition contracts that include security requirements and/or specifications versus the percentage of system and service acquisition contracts that do not include security requirements and/or specifications |
# NIST 800-55 Revision 1 Summary

<table>
<thead>
<tr>
<th>Revised</th>
<th>New</th>
<th>Remained</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Measures development methodology that ties into enterprise-wide strategic planning process</td>
<td>• Expanded the guide to address enterprise-level measurement and measurement within the SDLC</td>
<td>• Focus on using measures to gain insight into information security</td>
</tr>
<tr>
<td>• Expanded measures implementation methodology with integrated continuous monitoring</td>
<td>• Example information security measures addressing SDLC</td>
<td>• Importance of clearly defining and documenting the measures</td>
</tr>
<tr>
<td>• Measure development template</td>
<td>• Touch points with NIST Risk Management Framework</td>
<td>• Emphasis on use of measures to facilitate improvement of information security</td>
</tr>
<tr>
<td>• Mapping to NIST SP 800-53 Rev1 controls</td>
<td>• Overview of legislative and regulatory drivers (FISMA, GPRA, PMA)</td>
<td>• Types of measures</td>
</tr>
<tr>
<td>• Roles and responsibilities for consistency with FISMA and recent NIST publications</td>
<td>• Replaced <em>metrics</em> with <em>measures</em></td>
<td>• Implementation</td>
</tr>
<tr>
<td></td>
<td>• Example measures consistent with the updated template</td>
<td>• Effectiveness/Efficiency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Impact</td>
</tr>
</tbody>
</table>
Questions