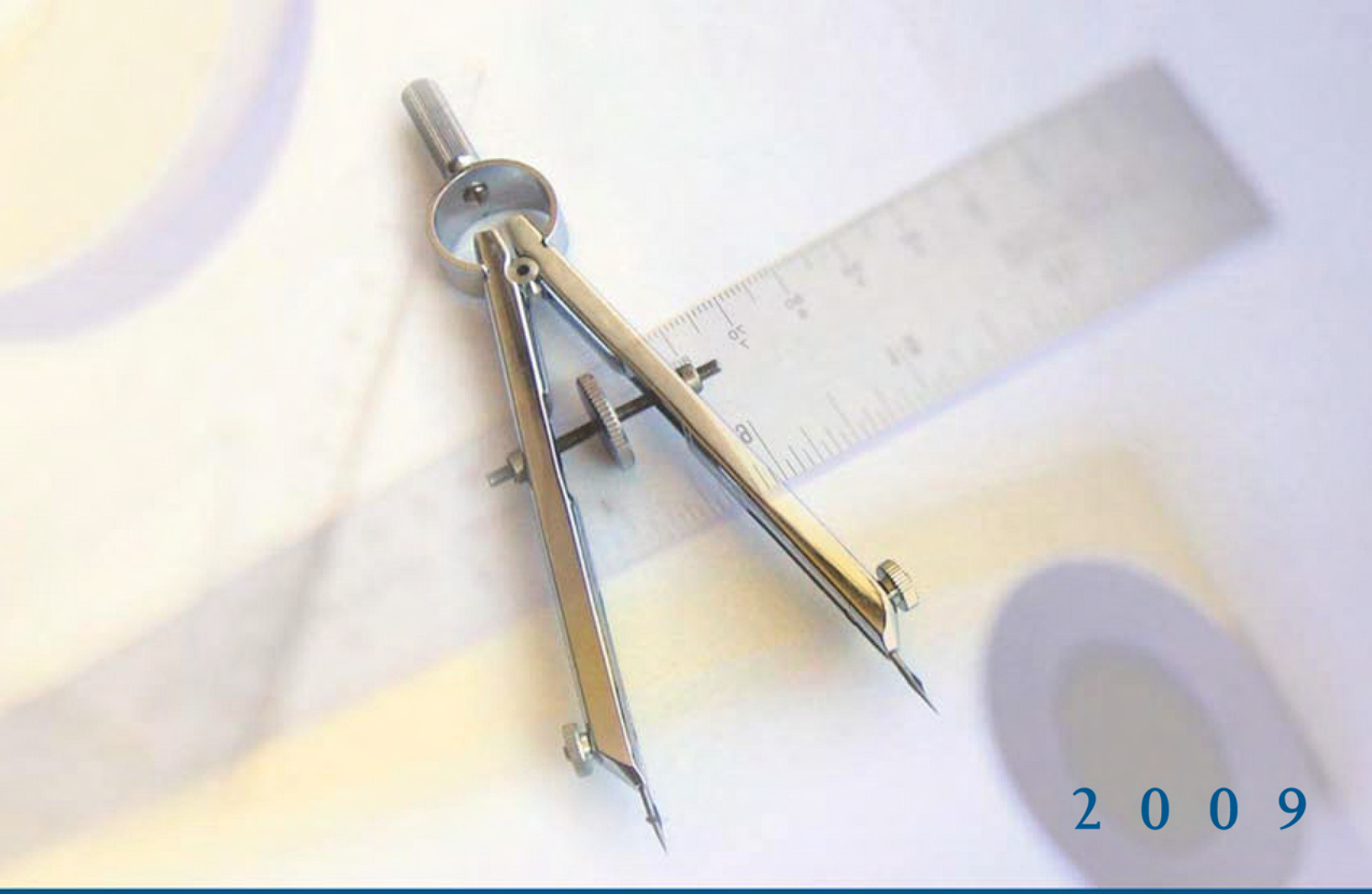

2009

# Interagency Security Committee
# Use of Physical Security Performance Measures

Homeland Security

# Table of Contents

## i. Preface

The Interagency Security Committee (ISC) originated by Executive Order 12977 after the Oklahoma City bombing of the Alfred Murrah Federal Building in 1995.The day after the attack, the President ordered an assessment of vulnerability of Federal facilities to terrorism or violence. The Vulnerability Report developed minimum physical security standards for civilian federally owned or leased facilities.

Protecting employees and private citizens who visit U.S. government-owned or leased facilities from all hazards is a complex and challenging responsibility. It is one of the top national priorities and the mission of the ISC.

In keeping with the authority provided in Section 5 of Executive Order 12977 and amended by Executive Order 13286, this document provides ISC policy, which requires Federal departments and agencies to use performance measurement and testing to assess physical security programs. This document outlines recommended guidance to Federal departments and agencies for implementing this policy. The guidance provides a basic performance model that measures inputs and accomplishments. It identifies the performance measurement cycle processes and provides examples of performance metrics for physical security. The ISC recognizes Federal departments and agencies will implement this policy and guidance in a manner reflecting the unique and varied mission requirements of their respective components.

## 1. Background

All major terrorist attacks in the United States (the Oklahoma City bombing, the two World Trade Center attacks, the attack on the Pentagon, and the Brentwood, Maryland anthrax attack) involved Federal facilities. Subsequently, many government facilities have received increased security funding in response to domestic and international terrorism. In several homeland security studies, the Government Accountability Office (GAO) concluded that much remains to be done to improve the overall management and protection of the Federal facility infrastructure. In two separate reports, the GAO identified policy and management issues specifically directed to the ISC. The GAO recommended the ISC promote key practices associated with the management of physical security programs (GAO 05-49), including the development and use of performance measurement.

In another study, the GAO found there is no government-wide guidance or standards for measuring facility protection performance (GAO 6-612). Without effective performance measurement data, the GAO said decision makers may not have sufficient information to evaluate whether their investments have improved security, reduced Federal facilities' vulnerability, and reduced the level of risk to an acceptable level. The GAO concluded the ISC should issue guidance applicable to all Federal departments and agencies on the use of performance measurement and testing procedures to assess the effectiveness of their security programs.

Measurement is an essential component of the requirements of the Government Performance and Results Act of 1993 (GPRA) and the Program Assessment Rating Tool (PART) from the Office of Management and Budget (OMB). GPRA requires a five-year strategic plan providing mission, goals, and a description of how the accomplishment of goals will be measured. PART is a tool by which the OMB assesses the effectiveness of an agency's or department's program based on responses to a series of questions generic to all programs. OMB rates the respective program as either *Effective*, *Moderately Effective*, *Adequate*, *Ineffective*, or *Results Not Demonstrated*, and then makes budget decisions accordingly. The GPRA and PART principles should be adhered to for internal goal setting, program assessment, and resource allocation.

## 2. Applicability and Scope

Performance measurement data is essential to appropriate decision making on the allocation of resources. Objective, unbiased information as to what is being accomplished, what needs additional attention (management focus and resources), and what is performing at target expectation levels, is vital to appropriate resource allocation decisions. Security counter-measures must compete with other program objectives for limited funding. Performance measurement tools offer security professionals a way to measure a program's capabilities and effectiveness and can help demonstrate the need to obligate funds for facility security.

### 2.1 Cautionary Note

While performance measurement and testing are necessary for effective management and oversight, they can become burdensome if senior management does not utilize them properly. GAO observed in a study (GAO-6-612) that "agencies face obstacles in developing meaningful, outcome-oriented performance goals and in collecting data that can be used to assess the true impact of facility protection efforts." Further, "in some programs, such as facility protection, outcomes are not quickly achieved or readily observable or its relationship to the program is

often not clearly defined." Without consistent management support, performance measurement and testing have the potential to become counterproductive and could evolve into ends in themselves rather than serving as a means of ensuring program success. Overcoming these obstacles will require sustained leadership, long term investment, and clearly defined performance goals, metrics and data. The costs associated with developing the initial requirements, particularly to establish performance databases, will require significant front-end funding. At the agency level, leadership must communicate the mission-related priority and commitment assigned to performance measurement actions. Management attention will be required at the facility level as well to ensure buy-in and cooperation among facility operators, security managers, building occupants, and other stakeholders. If management can meet these challenges, the physical security performance measures will help to ensure accountability, prioritize security needs, and justify investment decisions to maximize available resources.

### 2.2 Policy

Pursuant to Section 5 of Executive Order 12977, the following policy is hereby established for the security and protection of all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities.

Federal departments and agencies shall take the necessary action to comply with the following policies as soon as practicable:

- Federal departments and agencies shall assess and document the effectiveness of their physical security programs through performance measurement and testing.
- Performance measures shall be based on agency mission goals and objectives.
- Performance results shall be linked to goals and objectives development, resource needs, and program management.

## 3. Guidance

This guidance is provided to assist departments and agencies establish or refine a comprehensive measurement and testing program for assessing the effectiveness of their physical security programs. It is recognized that within large agencies or departments, security performance measurement and testing might best function at the major component organizational level (bureau, directorate, or office) and its field locations rather than at the senior management headquarters level. Nonetheless, senior management – the Chief Security Officer or equivalent – should ensure the consistent application and testing of performance measures throughout the agency or department.

## 4. Performance Measures

Performance measures can be categorized into three basic groups: input/process measures, output measures, and outcome measures. For consistency in the assessment of the effectiveness of physical security programs, the following definitions apply:

### 4.1 Input/Process Measures

Inputs are the budgetary resources, human capital, materials, and services, and facilities and equipment associated with a goal or objective. Process measures are the functions and activities undertaken that are geared toward accomplishing an objective.

### 4.1.1 Input/Process Measures Examples

The following are examples of input measures, including descriptions explaining how they relate to program assessment:

- **Asset Inventory**: This measure may encompass the entire facility asset inventory or a subset. For example, program managers could measure only those assets that have been (or need to be) assessed to those whose level of risk is acceptable. The inventory measure could also reflect various classifications, such as the ISC Facility Security Level (FSL) designations, or other mission-driven criteria, to establish priorities. Depending on the status, program managers should establish intermediate and long-term target objectives for the asset inventory for tracking and achieving long-term goals. An example of this is a measure indicating whether all assets have an acceptable risk rating.

- **Number of countermeasures in use**: Similar to the inventory of facilities, this measure provides a baseline for the number of countermeasures (by type) requiring maintenance, testing, or scheduled for replacement. This number may increase or decrease as the asset inventory fluctuates, or recurring risk assessments indicate the need for additional security equipment. As the number of countermeasures in use, increases, and the number of tested and repaired or replaced countermeasures increases, the acceptable risk rating should also increase for your asset inventory as suggested in the first example.

- **Resource Requirements**: These measures track the resources required to accomplish the security program mission:
    - Full-Time Equivalent (FTE) employees, contract support, and training;
    - FSL determinations and risk assessments;
    - Countermeasure installation, maintenance, testing, evaluation and replacement; and
    - Overall Security Program Management (salaries, IT cost, administrative cost).

  Tracking the resources applied to physical security efforts provides program managers with an understanding of the necessary resources, including expenditures and personnel, required for effective physical security program operations. Program managers can use this information to determine program growth, increases in cost, efficiency gains, and output costs. Essentially, this information provides an overview of the resources required to achieve program goals and to accomplish overall program mission goals. When considered in conjunction with output and outcome measures, they help determine the benefit of using various resource levels. Moreover, program managers should use this information to plan and justify resource requirements for future efforts.

## 4.2 Output Measures

Outputs are the products and services produced by the organization and generally can be observed and measured. Efficiency is a measure of the relationship between an organization's inputs/processes and its outputs.

### 4.2.1 Output Measures Examples

The following are examples of output measures and how they relate to assessing program effectiveness:

- **Security assessments completed versus planned:** A core component of a physical security program is the scheduling of initial and recurring risk assessments and the accompanying FSL determination. Every agency or department should have an established schedule for assessing each facility. Tracking and measuring the percentage of completed assessments versus what was planned for the year, by quarter, or other period indicates management's commitment to maintaining an organized and efficient physical security program. More importantly, risk assessments performed on a regular schedule provides a means of effectively addressing changes in threats and vulnerabilities, and corresponding countermeasure needs. A typical target objective would be to complete a specific number of assessments annually, based on a planned schedule.

- **Countermeasures deployed**: This measure reflects how well the deployment of countermeasures is managed throughout the procurement, installation, and acceptance cycle. Once funding has been made available, target dates (e.g., a specific date, month, or quarter) should be established. This target date is then compared with the actual deployment "date." If there is no existing data available for projecting a reasonable target date, a baseline should be established using representative countermeasures to determine the typical time frame for deployment of various kinds of countermeasures. This enables the manager to reasonably project target dates for future countermeasures. A typical target objective for this measure may be to deploy all fully-funded countermeasures on time (on or prior to the scheduled date) 95 percent of the time. The 5 percent margin of error allows for unforeseen events or circumstances that could not have been reasonably anticipated when the target dates were initially established. Once actual results are achieved, incremental improvement target dates may be necessary until the processes, planning, and scheduling procedures can be refined to ensure successful deployment 95 percent of the time. Note: *This measure encompasses capital investments facility enhancements and equipment, new process changes, and countermeasure activities. Separate reporting is encouraged for each of these categories since the responsibility for each may differ, and corrective process improvements vary, among the organizational elements involved.*

- **Countermeasures tested:**[1] This measure focuses on accomplishing an established schedule for testing countermeasures to determine how well they are working. Testing encompasses such elements as determining whether or not equipment is calibrated properly, security guards are knowledgeable in post order procedures, and intrusion detection systems (IDSs) are activating properly. For critical infrastructure, testing may include planned exercises to breach security to ensure existing countermeasures are capable of securing the facility against the most sophisticated attempts to illegally access the facility. All testing should be based on an established set of testing protocols. Because individual facilities may have numerous countermeasures in place, it is unrealistic to attempt to test all countermeasures annually. Random sampling may be necessary for larger facilities.

[1] **Testing -** Encompasses those procedures used to assess the performance of security equipment, security guards, and emergency planning and response. Security equipment testing includes, but is not limited to, alarm/detection systems testing, examining equipment calibration, detection of training weapons and other simulated contraband, and appropriate positioning of surveillance equipment.

- **Incident Response Time:** This measure is suitable for a number of security related requirements but only when the security manager has operational control over response capability, or has negotiated a service agreement with a response provider. Use of this type of measure usually requires a baseline assessment of existing average response times. This average should be compared with a benchmark or desired standard. If there is a high volume of incidents within a given facility inventory and there is no automated time recording database available, random sampling of incidents may be necessary. Sampling should be large enough to reflect normal operational circumstances. Incremental performance target objectives may be necessary to guide development of improved procedures and future funding needs.

## 4.3 Outcome Measures

Outcomes or results represent the impact of the organization upon its customers or problems. Results are often classified in terms of the achievement of a desired condition, the prevention of an undesired condition, or user satisfaction. Effectiveness is a measure of the relationship between an organization's inputs/processes and outcomes/results.

### 4.3.1 Outcome Measures Examples

Outcome measures are used to assess the cumulative results of output activities in achieving objectives and indicate how well individual tasks or target objectives contribute to the accomplishment of broad-based security program goals. Outcome measures may also support more than one program objective or goal. Examples include:

- **Facility Asset Inventory Secured (Strategic Goal):** This measure reflects the cumulative impact of reducing individual facility risk levels through the deployment of security countermeasures throughout the asset inventory. The strategic goal is to achieve and sustain an acceptable risk rating for all facilities. Tracking this strategic goal is a multi-year process. The risk rating is reflective of countermeasures in place and working properly throughout the inventory. An acceptable risk rating may be defined based on a scoring system for evaluating the perimeter, facility envelope, and interior security features of an asset, or it could be simply defined as being ISC standard compliant.
- **Emergency Preparedness (Strategic Goal):** This measure focuses on the degree to which employees and senior management are trained and perform up to expectations in emergency training exercises. It reflects the cumulative results of Continunity of Operations Plan (COOP) activation training exercises, Occupant Emergency Plans (OEP) drills, and other emergency exercises. Assuming all output measure target objectives are met, a typical strategic outcome goal for this measure might be to achieve an overall 98 percent success rate in accordance with expected behaviors.
- **Program Efficiency (Program Goal):** This outcome measure is intended to capture the cumulative effect of individual process efficiency initiatives (outputs). A typical long- term goal might be to limit overall security program cost increases to a vairable percentage per year. The results of individual efficiencies must be tracked, recorded, and summed.

## 4.4 Note on the Examples

The examples included above are provided for agencies as they develop or refine their performance measurement program. They may be adopted or modified to meet their particular mission and program needs. Departments and agencies should utilize only those measures suitable to and supportive of their particular physical security program. Variances within department or agency components in both number and content may also be appropriate due to program or budgetary constraints. In short, the examples below are provided to assist departments and agencies, and their components, in developing the measures that best suit their needs. Additional comments can be found in Appendix A.

## 4.5 Performance Measurement Process Chart

The following chart (Table 1) illustrates how the process of using performance measures ties to mission, goals, objectives, specific actions (outputs), and outcomes. This hypothetical example is based on the mission of securing all facilities and a goal of ensuring all facilities comply with ISC security standards within 36 months. To achieve the goal, two program objectives were established. The first objective is to assess all 100 of the hypothetical agency facilities within 18 months; the second is to deploy all approved security measures identified in those assessments within 18 months after the last assessment is completed. The chart identifies several tasks or actions required to accomplish the objectives, but they should not be viewed as all-inclusive. In the example, the results indicate some slippage, but overall, the delay in approving all recommended countermeasures did not adversely affect the accomplishment of the goal within the target timeframe. The bottom portion of the process chart shows how the input, output and outcome measures support each phase of the process and ultimately the goal of ensuring all facilities are ISC compliant within 36 months was achieved.

| **Mission: Secure Facilities** | **Goal:** Ensure all [agency] facilities are ISC compliant within 36 months. | |
|---|---|---|
| **Objectives** | **Actions** | **Results** |
| 1. Assess all 100 [agency] facilities for compliance within 18 months | 1. Complete all scheduled risk assessments on time (quarterly schedule)<br>2. Obtain consensus/ approval on recommended corrective measures (CMs) within 45 days of risk assessment | 100% of risk assessments completed on time. 18 compliant facilities<br><br>90% of recommended CMs approved within 45 days (Remaining 10% approved within 60 days.) |
| 2. Implement corrective measures as needed within 18 months of last assessment | 1. Identify priority CMs, and coordinate as appropriate with facility managers<br>2. Award ID/IQ contract(s) for CM installation<br>3. Conduct post deployment<br>4. ISC compliance inspection | 250 CMs identified as needed to make facilities ISC compliant<br><br>Five ID/IQ contracts awarded to install 250 CMs in 82 facilities within 18 months of last risk assessment<br><br>All CMs installed and validated |

| Inputs | Outputs | Outcome |
|---|---|---|
| Inputs:<br>1. Necessary travel and support funding budgeted<br>2. Quarterly risk assessment schedule developed with dates.<br>3. Estimated CM purchase and installation funding budgeted<br>4. CM installation plan developed and approved (multiple ID/IQ contracts) | Outputs:<br>1. 100 approved assessments<br>2. Approved CMs prioritized<br>3. CMs deployed within 18 months of last risk assessment<br>4. Post CM deployment inspection reports completed | Outcome:<br>1. All 100 [agency] facilities are ISC compliant within 36 months<br><br>*Goal achieved* |

*Table 1: Performance Measurement Process Chart*

## 5. Performance Measurement Implementation

Performance measures are a useful tool for decision makers at all levels. Program managers at the agency headquarters level use performance measures to determine if their security program is accomplishing or supporting agency mission, goals, and objectives. Field level managers may use performance measures to demonstrate program effectiveness to stakeholders, assess emergency preparedness capabilities, oversee security equipment maintenance and testing programs, and determine the adequacy of resources to support operational security requirements. Physical security related performance measures provide valuable information used to support funding requests, accomplish program goals and identify areas for improvement, and process change or additional training.

### 5.1 Headquarters and Field Level Interaction

Implementing a performance measurement program at the agency level is required to link the specific measures to the agency's established goals. Generally, a strategic plan contains one or more goals, which impacts or requires the direct support of the physical security program operations, over a multi-year time span. Therefore, performance measurement initiatives at the agency headquarters level are also generally multi-year efforts with phased implementation aligned with the agency strategic plan. At the field level, performance measurement activities must support the agency level goals and objectives. However, they may include measures aimed at assessing and demonstrating the effectiveness of the security program at the local level in ways different from the agency program measures. These field performance measures may be short term or multi-year initiatives.

The Performance Measurement Process Chart (Table 1) illustrates the implementation of an agency headquarters level goal [ensure all facilities are ISC compliant within 36 months] with two supporting objectives [assess 100 facilities within 18 months and implement corrective measures within 18 months of the last assessment]. These two objectives support the goal of achieving ISC compliance with a three-year timeframe for the entire organization. At the field level, the security program manager may be heavily involved in conducting the risk assessments and, once funding is available, implementing the approved countermeasures. The security program manager may also be involved in measuring the time and resources needed to complete individual assessments or the time required to obtain full approval of recommended countermeasures. This information may be helpful in justifying additional resource requirements necessary to meet the headquarters assessment schedule or to initiate process changes to reduce

approval timeframes. The security program manager may track the accuracy of countermeasure deployment costs compared to the budget provided by headquarters. This will provide valuable information in developing input measure data for preparing a future budget submission.

The field manager may also establish local objectives. For example, the manager may establish a performance objective to develop and issue revised guard orders addressing the use of the new security equipment recommended in the required risk assessments. This output measure could be based on measuring the planned versus actual issuance date, using the date of countermeasure deployment as the planned date. Another example of a field manager establishing a performance measure is testing existing countermeasures to ensure they are working properly, such as setting a goal of 99 percent effectiveness. Testing confirms reliability, or lack thereof, of maintenance programs, ensures credibility with facility occupants, and provides empirical data to support countermeasure replacement if necessary, all of which would be essential to support the conclusion that all facilities are ISC compliant. Whether the performance measures are driven by agency headquarters goals or field manager initiatives, all performance measures should provide a basis for assessing program effectiveness, establish objective data for resource and process improvements, and lead to overall security program effectiveness.

Goals and objectives established at the headquarters or field level, illustrates the effective use of performance measures that requires a collaborative effort. The team should be led by the security professional but should include budget, procurement, and facility management officials and, where appropriate, human resource and training officials. Each participant should be fully briefed and share a common understanding of the measurement initiative, including an understanding of the actual measures, definition of terms, data sources, and most importantly, a commitment to utilize the results to improve program performance.

## 6. Conclusion

The guidance in this document provides the foundation for a measurement program that will endure both in terms of the metrics themselves and, more importantly, the use of performance measurement as a management tool. The use of performance measurement and testing is one of six key management practices the ISC is promoting within the Federal physical security community. Combined with future ISC management documents, ISC membership seeks to achieve consistent, professional, and cost effective management of physical security programs across the Federal government that improve the protection of and security within Federal facilities.

To assist in the development of a physical security performance measurement program, Appendix B in this document includes an annotated bibliography of source documents.

# 7. References

## 7.1 Appendix A: Quick Reference Guide

| Type | Category | Example | Purpose |
|---|---|---|---|
| **Input/Process Measures** | Asset Inventory | Number of facilities, Number assessed, Number at Acceptable Level of Risk | Program scope identification |
| | Countermeasures in Use | CM Inventory by type: guards, surveillance systems, magnetometers, x-rays, canines, blast protection, vehicle barrier protection, etc. | Program scope, resource development, CM repair/replacement cost base, testing inventory |
| | Resources Requirements | FTE (number and salary), FSL and risk assessment workload; countermeasure procurement, installation, maintenance, and testing costs , database expense, contract support, training, travel, contract security guards, equipment | Oversight, program management, efficiency targets, trends/projections |
| | Process Governing Approval of Facility Security Assessment (FSA) | Track time and costs from initial completion to final approval of the FSA recommendations | To maximize efficient use of resources (human capital) |
| **Output Measures** | Security Assessments Completed | Percentage of planned assessments completed within the timeframe | Program management (annual target objective), stakeholder communication |
| | Level of Risk | Number/Percentage of facilities at acceptable risk levels (e.g., ISC compliant), annual target/incremental improvement | Program management, stakeholder communication |
| | Countermeasures Deployed | Installation/deployment schedule, (percentage of planned completed by target date); track procurement, installation, and acceptance progress | Program management; stakeholder communication |
| | Countermeasures Needed (backlog) | Inventory of new and replacement countermeasures (annual backlog reduction target) | Program management |
| | Countermeasures Tested | Testing schedule, (percentage passing vs. failed) annual target leading to long-term performance objective | Program management; assessment validation |
| | Response Time | Time required for responders (guard, law enforcement, emergency response technician) to arrive/initiate response protocol | Program management, response readiness, stakeholders trust/confidence |
| | Emergency Exercises | OEP, COOP exercises (actual vs. expected behaviors); after action report assessment | Emergency response enhancement, program management, stakeholder communication |

| | | | |
|---|---|---|---|
| | Stakeholder Satisfaction | Tenant or customer satisfaction assessment (survey); annual improvement targets | Program assessment, stakeholder confidence, identification of areas needing improvement |
| | Development and Training | 1. Staff development (scheduled training vs. actual)<br>2. Customer training (crime awareness, security training) planned vs. actual | Program development; stakeholder communication and feedback |
| **Outcome Measures** | Inventory Secured | All facilities are protected to an acceptable risk level rating and are ISC compliant | Strategic goal accomplishment, facilities equipped with adequate countermeasures |
| | Security Measures Working | Security countermeasure inventory working at strategic goal level | Strategic goal accomplishment; security measures are effective |
| | Emergency Preparedness | Employees, contractors, senior management trained and prepared to response to emergency incident | Strategic goal accomplishment, OEP, COOP Plans validated and employees prepared based on successful training |
| | Incident Reduction | Security violations, thefts, vandalism reduced | Strategic goal accomplishment; inventory experienced fewer security violations, etc |
| | Program Efficiency | Physical Security program operating more efficiently | Strategic goal accomplishment; mission accomplished within resources/more cost effective delivery |

## 7.2 Appendix B: Annotated Bibliography

The following reflect publications reviewed in preparing this document. They assist the physical security manager in developing a physical security measurement and testing program.

1. **Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices**, Government Accountability Office, GAO-05-49, November 2004.
   Document reflects GAO's review of the progress made in coordinating the government's facility protection efforts. It recommended the ISC develop an action plan to guide future initiatives and that it promotes key management practices, one of which is performance measurement.
2. **Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts**, Government Accountability Office, GAO-06-612
   Document reflects GAO's review of physical security performance measurement and testing practices at Federal agencies, State, and local governments, private industry, and foreign countries. The GAO found no standards governing physical security measures and recommend the ISC develop such guidance for Federal agencies.
3. **Performance Measurement and Evaluation**, Government Accountability Office, GAO-05-739SP, May 2005.
   Document provides definitions and summarizes the relationships between performance measurement and program evaluation including outcome evaluation, impact evaluation and cost-benefit and cost-effective analyses.
4. **National Infrastructure Protection Plan (NIPP)**, Department of Homeland Security, 2006, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
   The NIPP provides a comprehensive risk management framework that can apply across all 18 Critical Infrastructure and Key Resource Sectors to enhance protection of the Nation's vital assets.
5. **Government Performance Results Act of 1993,** www.whitehouse.gov/omb/mgmt-gpra/gplaw2m.html
   Law establishes the requirements for Federal departments and agencies to submit a 5-year strategic plan with mission goals as well as, methods used to accomplish strategic goals. It focuses on budget and performance integration.
6. **Program Assessment Rating Tool (PART),** www.whitehouse.gov/omb/part.
   First initiated in 2002 for the FY 2004 budget cycle, the PART is a tool used by OMB to assess program performance to include program management, measurement, and program results.
7. **ExpectMore.gov**, Office of Management and Budget (OMB), www.whitehouse.gov/omb/expectmore/
   OMB provides results of ratings for all Federal programs.
8. **Measures and Metrics in Corporate Security**, George K. Campbell, Security Executive Council Publication Series, 2006, www.csoexecutivecouncil.com.
   Document provides guidance in development of a metrics program that aligns with business goals.
9. **A Background Paper on Measuring Police Agency Performance**, Edward R. Maguire, Ph.D., George Mason University, Commissioned by the Commission on Accreditation For Law Enforcement Agencies, Inc., May 1, 2003.

Document provides guidance in developing "comparative performance measures" for police organizations to compare organizations or multiple agencies over time.

10. **The Implausibility of Benchmarking Police Performance,** James R. Brunet, Department of Public Administration, North Carolina State University.
    This document discusses the difficulties in using traditional police performance measures and suggests alternatives for better managing police performance.
11. **Disaster Exercise Management, Part 1: Performance Measurement**, William F. Comtois, www.SecurityIntoWatch.com.
    This document discusses the need for and the value of performance measurement in conducting disaster exercises to better prepare of emergency incidents.
12. **Annual Performance Progress Report (APPR) for Fiscal Year 2005-06**, Oregon Department of Energy, October 16, 2006, http://oregon.gov/ENERGY/ProgRept.shtml
    This report provides on overview of how the Oregon Department of Energy develops and uses performance measures.
13. **Performance Data and Analysis, Part 2 FY 2006 Performance and Accountability Report**, Department of the Interior, www.doi.gov/pfm/par/par2006.
    This report provides important financial and performance information for the Department of the Interior (DOI). It is DOI's principal publication and report to Congress and the American people on the stewardship, management, and leadership of the public funds entrusted to DOI.
14. **OMB Circular No. A-123 Management Responsibility for Internal Control,** December 21, 2004, www.whitehouse.gov/omb/circulars/a123/a123_rev.html.
15. **Federal Preparedness Circular 65 (FPC 5),**www.fema.gov/pdf/library/fpc65_0604.pdf.

# Interagency Security Committee Participants

## ISC Chair

**James Snyder**
**(Acting Chair)**
**Deputy Assistant Secretary for Infrastructure**
**U.S. Department of Homeland Security**

**ISC Executive Director**
**Austin L. Smith**
U.S. Department of Homeland Security
Office of Infrastructure Protection

**Working Group Chair**
**Mark Strickland**
Security Specialist
Administrative Office of the U.S. Courts
Court Security Office

## Working Group Members

**Gwainevere C. Hess**
Senior Policy Analyst
U.S. Department of Homeland Security
Office of Infrastructure Protection

**Joseph Gerber**
Physical Security Specialist
U.S. Department of Homeland Security
Office of the Chief Security

**Acknowledgement**

*This working group acknowledges the work of Mr. Mark Harvey (Federal Protective Service) on the first draft of the Performance Measures document.*