

# **Getting Started with Security Metrics: Guidance from the I3P**

**Cliff Glantz (Pacific Northwest National Laboratory)**

**Martin Stoddard (PNNL)**

**Lori O'Neil (PNNL)**

**Nino Zuljevic (PNNL)**

**Deb Bodeau (MITRE)**

**Annie McIntyre (SNL)**

**Blair Becker (SNL)**

**Joost Santos (UVA)**

**Bayard Gennert (UVA)**

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

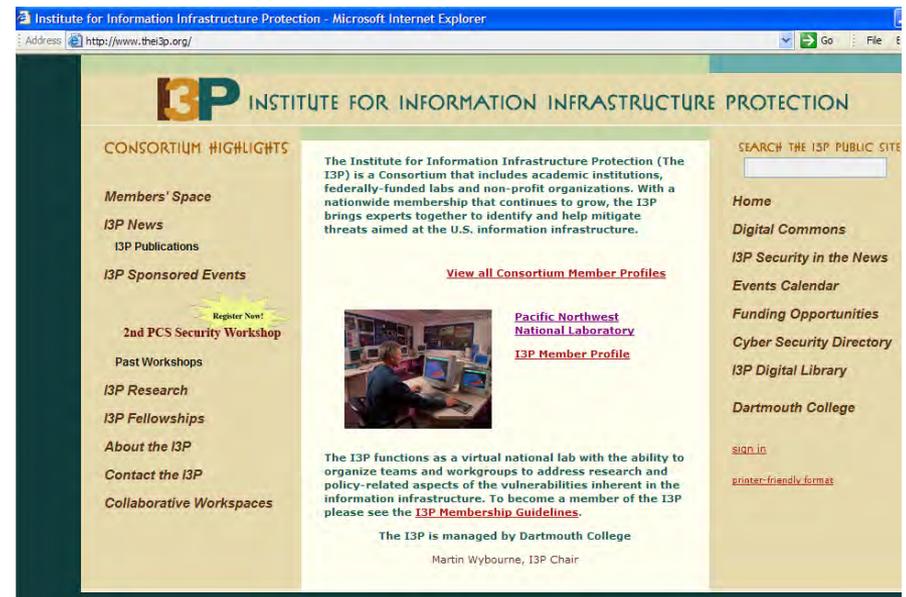
# Overview

- ◆ Introduction
- ◆ What's being done?
- ◆ What's can you use to get started?
- ◆ What tools can we give you to use?
- ◆ What can you do – now and in the future?



# The Institute for Information Infrastructure Protection (I3P)

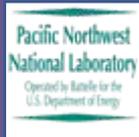
- The I3P is a consortium of academic institutions, federally-funded labs, and non-profit organizations. (see [www.theI3P.org](http://www.theI3P.org))
- The I3P organizes multidisciplinary teams to do technical and policy-related research on issues involving vulnerabilities in information infrastructure.



# The I3P SCADA Security Project

- ◆ The *I3P SCADA Security Project* is investigating ways to enhance PCS security
- ◆ Our initial focus is on the oil and gas sector
- ◆ Eleven institutions recognized for their expertise in cyber security and critical infrastructure protection research are participating on this I3P project (Dartmouth, SNL, PNNL, SRI, MITRE, UVA, NYU, U-Tulsa, MIT-LL, UIUC, and the I3P).

# I3P PCS Security Metrics Team



## Pacific Northwest National Laboratory

Cliff Glantz – Lori Ross O’Neil – Wayne Meitzler – Nino Zuljevic

CVO

Marty Stoddard



## Sandia National Laboratory

Annie McIntyre – Blair Becker – Mary Young



## University of Virginia

Joost Santos – Bayard Gennert



## The MITRE Corporation

Deb Bodeau

# The Importance of Measurements

*“If you can’t measure it, you can’t manage it.”*

Some questions that decision makers are asking:

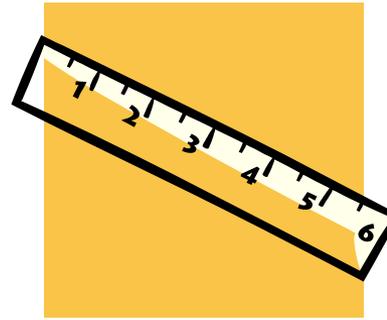
- ◆ Is our security posture adequate for the risks we face?
- ◆ Does our security posture comply with standards and how does it compare with industry best practices?
- ◆ Is our security posture improving or getting worse?
- ◆ What are the costs/benefits of investments in security?

# Measurements

- ◆ A measurement can quickly reveal aspects of a system or process that are not inherently obvious.
- ◆ This measurement can be in the form of a number, trend line, relative position with respect to a set point, etc.
- ◆ However, in many instances measurements by themselves may have little meaning.



# What is a Metric?



## Definitions:

- ◆ metric: *“Of or relating to the meter or the metric system”*
- ◆ metrics: *“The use or study of metrical structures in verse”*

– American Heritage Dictionary

## Digging deeper:

- ◆ *“a mathematical function defined for a coordinates system that assigns a value to each pair of elements equal to the distance between them, or to a property analogous to distance between points on a line”*

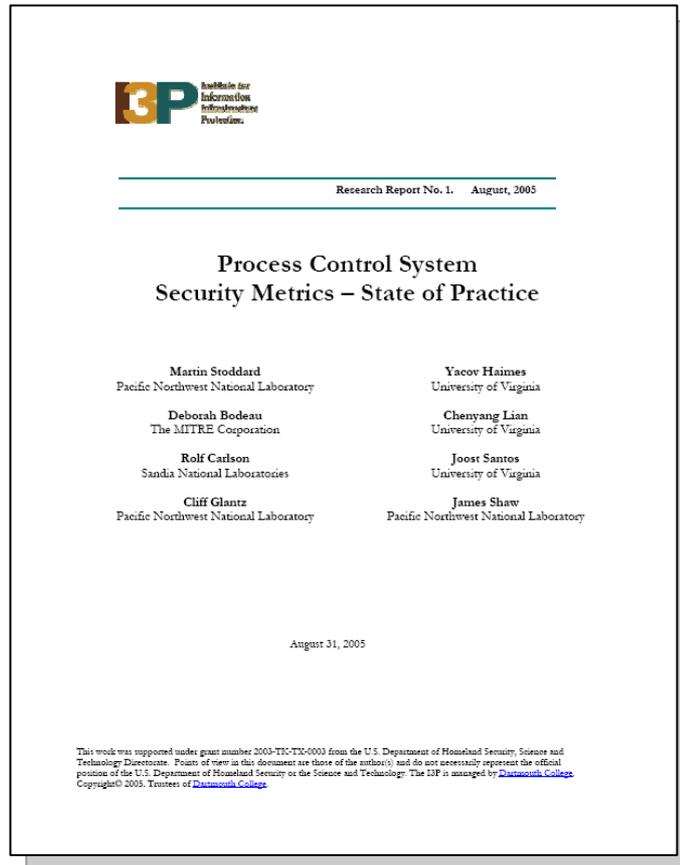
– Encarta Dictionary

# Metrics

- ◆ *Metrics are measurements that are compared to a known scale or benchmark to produce a meaningful result.*
- ◆ Metrics are tools that enable stakeholders to make decisions based on qualitative or quantitative assessments rather than best guesses.
- ◆ We found that in the oil and gas sector (and other sectors as well) the availability and use of metrics to address PCS security issues is quite limited.



# PCS Security Metrics: State of Practice



- Published in August, 2005
- Reviews existing metrics systems, standards, and scoring tools that have the potential to be applied to PCS in the oil and gas industry
- Presents an overview of risk assessment techniques and risk filtering and ranking metrics
- Describes the challenges and ongoing efforts for developing new metrics tools

See I3P Research Report #1 at  
<http://www.thei3p.org/publications/>

# State of Practice: IT Security Metrics

- ◆ Well-established standards of good practice
  - ISO/IEC 17799
  - FIPS 199 & 200, NIST SP 800-53, other NIST publications
- ◆ Guidance on defining metrics and creating metrics programs
  - DRAFT NIST SP 800-53A (assess control effectiveness)
  - DRAFT NIST SP 800-80 (create metrics program)

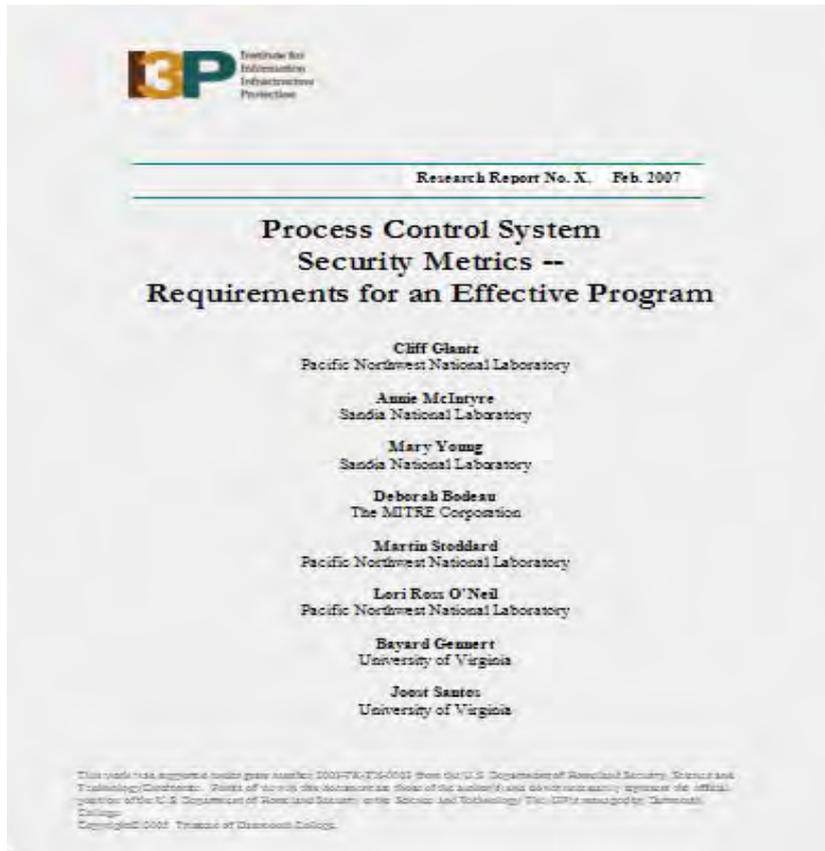
# State of Practice: PCS Security Metrics

- ◆ Increasing definition of standards of good practice
  - ANSI/ISA-TR99.00.01, *Security Technologies for Manufacturing and Control Systems*
  - API-1164, *Pipeline SCADA Security*
  - DRAFT NIST SP 800-82, *Guide to SCADA and Industrial Control System Security: Recommendations of the NIST*
  - DOE 21 Steps to Improve Cyber Security of SCADA Networks
- ◆ Increasing guidance on defining metrics and creating metrics programs
  - ANSI/ISA-TR99.00.02, *Integrating Electronic Security into the Manufacturing and Control System Environment*
  - I3P Research Products

# PCS Security Metrics (cont)

- ◆ Tools and technologies for producing measurements and metrics are needed
- ◆ PCS security metrics continue to be a recommended research topic
- ◆ Research is looking at relationships between PCS security metrics, enterprise risk assessments, and critical infrastructure security assessments

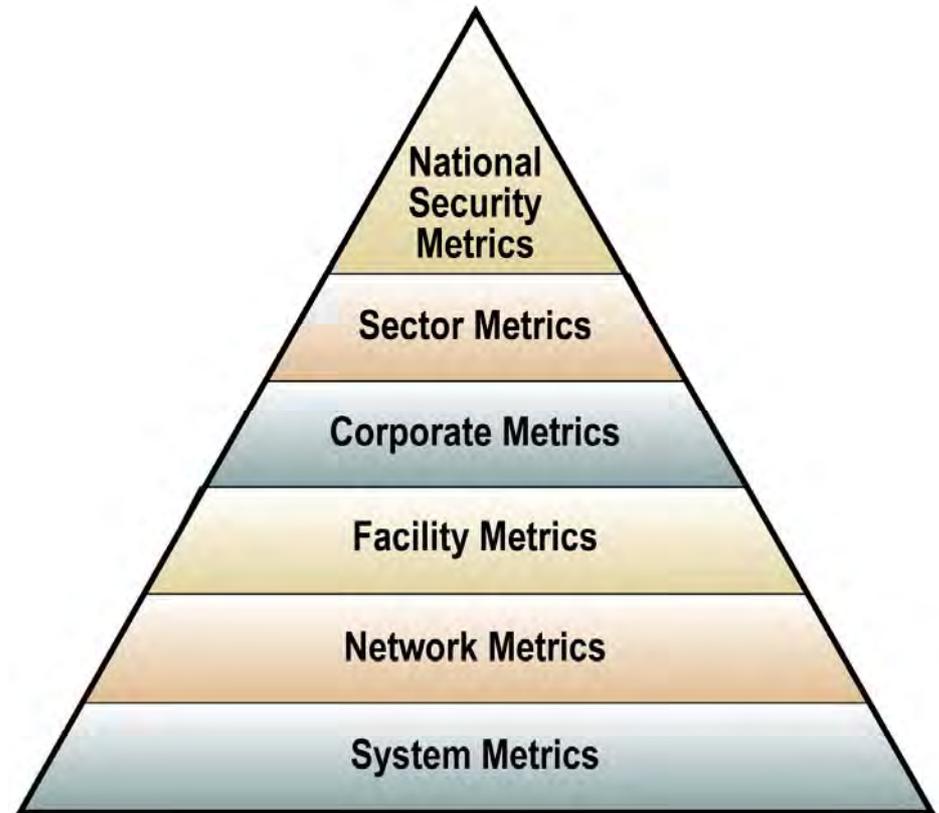
# Requirements for an Effective Program of Security Metrics



- ◆ Nearing publication
- ◆ Lays out the case for using security metrics
- ◆ Provides basic guidance for developing a metrics program
- ◆ Provides a framework for developing metrics
- ◆ Where and when to use metrics

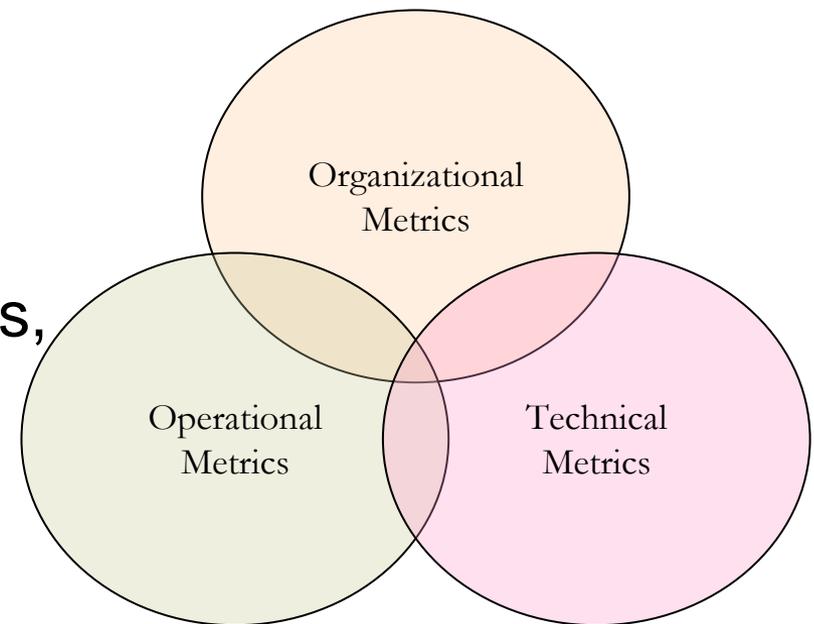
# A Key Basic Concepts

- ◆ Select metrics that are tailored to where they will be used
  - At the pinnacle we have metrics used by national decision makers
  - At the base we have metrics used by process control system operators



## Key Concepts (cont)

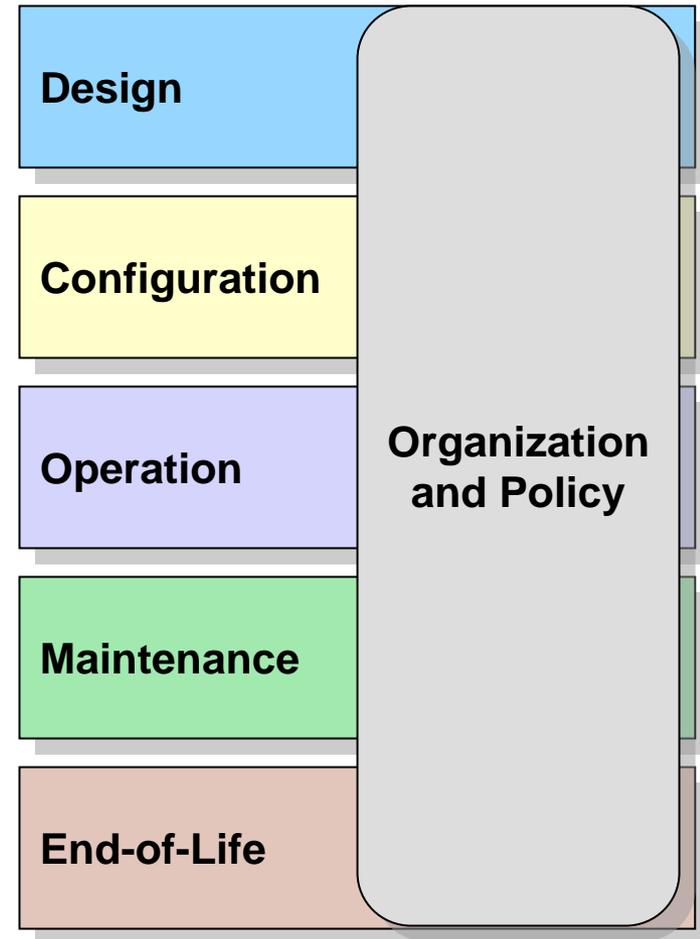
- ◆ Select a set of metrics that cover important *operational*, *organizational*, and *technical* areas of concern
- ◆ Metrics should cover security policies, procedures, practices, and performance
- ◆ Metrics that don't cover all of the major areas may give a misleading indication of security performance



# Key Concepts (cont)

Metrics should be used throughout the PCS lifecycle:

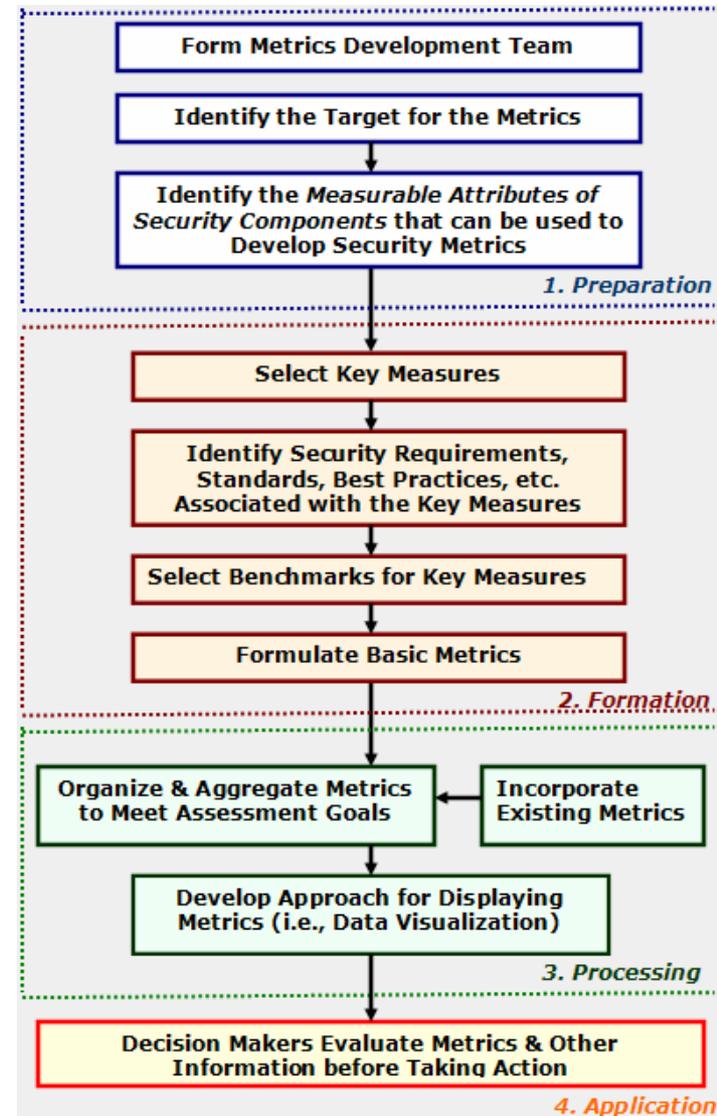
- Organization and Policy
- Design
- Configuration
- Operation
- Maintenance
- End-of-Life



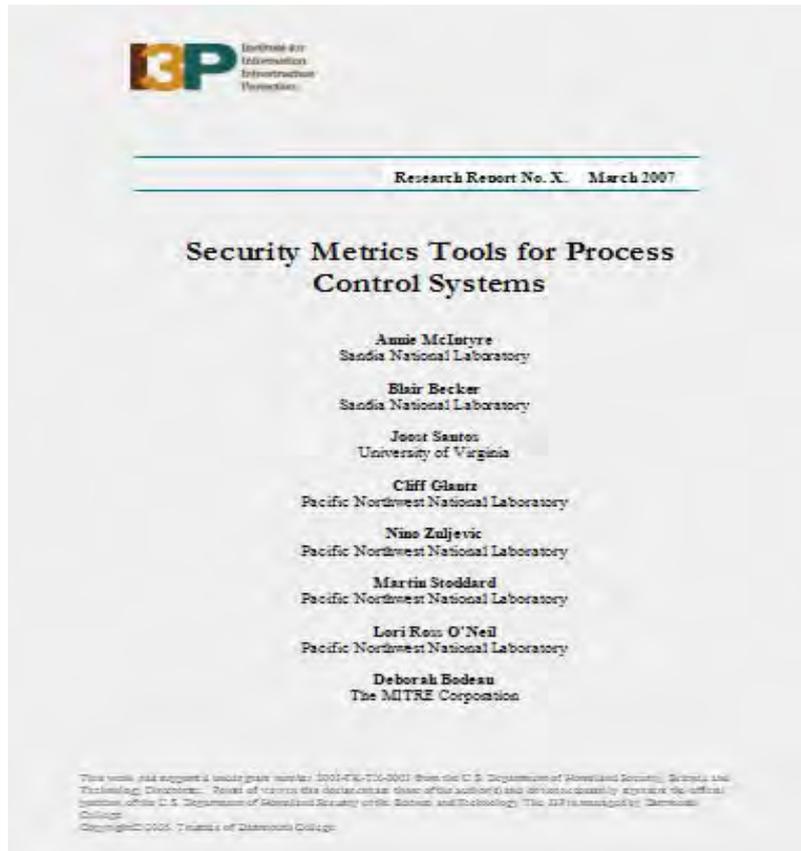
# Key Concepts (cont)

Use a metrics development framework to design and select your metrics. Stages in the framework include:

1. Preparation
2. Formation
3. Processing
4. Application



# Security Metrics Tools



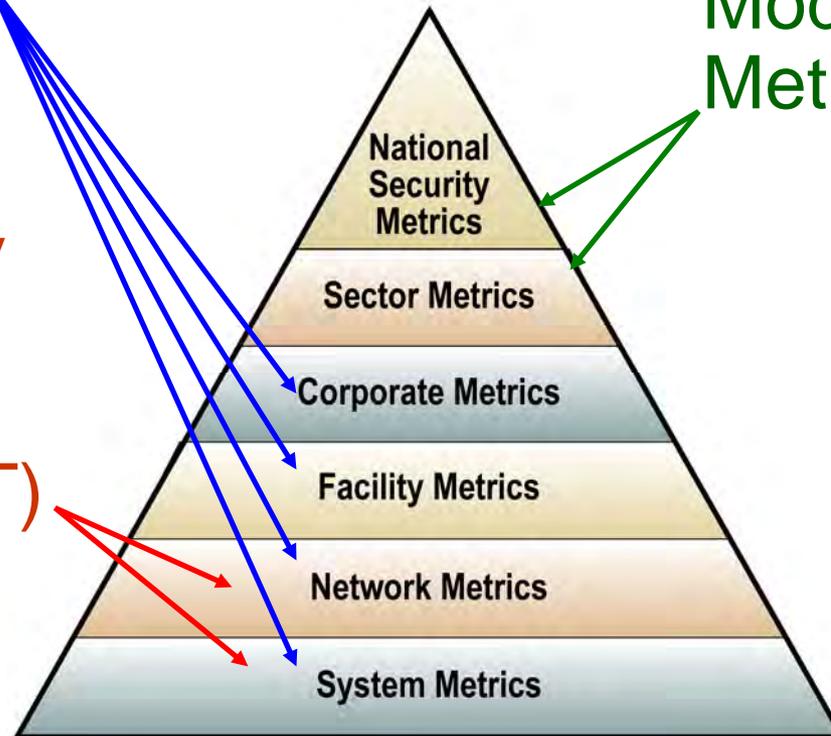
- ◆ Report in draft form
- ◆ Describes security metric tools developed by the I3P
- ◆ Describes other available security metrics tools
- ◆ Provides examples of how to apply metrics tools

# Overview of I3P Security Metrics Tools

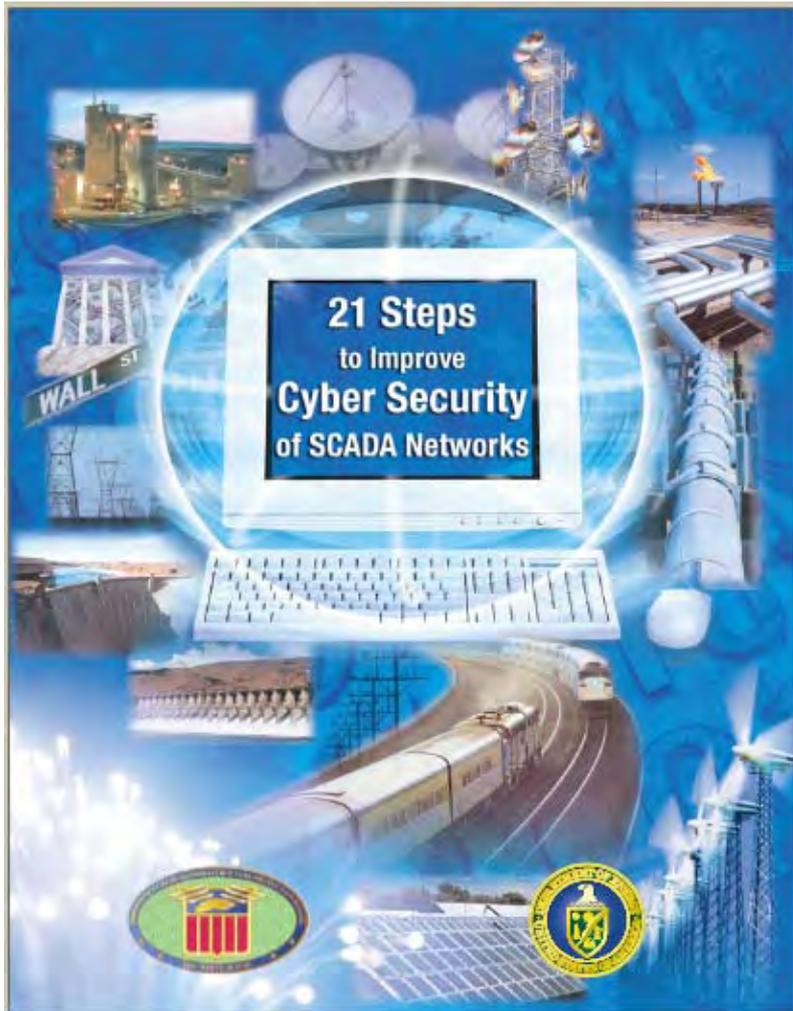
DOE 21 Steps  
Metrics Tool

PCS Security  
Technical  
Evaluation  
Tool (P-STET)

Inoperability  
Input-Output  
Model (IIM)  
Metrics



# 21 Steps Metrics Tool



- ◆ In 2002, the President's Critical Infrastructure Protection Board and the Department of Energy developed 21 Steps to Improve Cyber Security of SCADA Networks
- ◆ Provides basic steps to an organization can take to improve the security of their SCADA networks.

The following steps focus on specific actions to be taken to increase the security of SCADA networks:

### 1. Identify all connections to SCADA networks.

Conduct a thorough risk analysis to assess the risk and necessity of each connection to the SCADA network. Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected. Identify and evaluate the following types of connections:

- Internal local area and wide area networks, including business networks
- The Internet
- Wireless network devices, including satellite uplinks
- Modem or dial-up connections
- Connections to business partners, vendors or regulatory agencies

### 2. Disconnect unnecessary connections to the SCADA network.

To ensure the highest degree of security of SCADA systems, isolate the SCADA network from other network connections to as great a degree as possible. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the SCADA network must be a primary goal to provide needed protection. Strategies such as utilization of “demilitarized zones” (DMZs) and data warehousing can facilitate the secure transfer of data from the SCADA network to business networks. However, they must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

### 3. Evaluate and strengthen the security of any remaining connections to the SCADA network.

Conduct penetration testing or vulnerability analysis of any remaining connections to the SCADA network to evaluate the protection posture associated with these pathways. Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the SCADA network. Since the SCADA network is only as secure as its weakest connecting point, it is essential to implement firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access from and to the SCADA network, and be as specific as possible when permitting approved connections. For example, an Independent System Operator (ISO) should not be granted “blanket” network access simply because there is a need for a connection to certain components of the SCADA system.

# Steps 1-10

Focus on actions to increase security of SCADA networks:

- ◆ Identify all connections to SCADA Networks
- ◆ Disconnect unnecessary connections to the SCADA network
- ◆ Evaluate and strengthen the security of remaining connections...

# Steps 12-21

Focus on management actions to establish an effective cyber security program:

- ◆ Clearly define cyber security roles, responsibilities, and authorities...
- ◆ Document systems that serve critical functions or contain sensitive information that require additional protection...

The following steps focus on management actions to establish an effective cyber security program:

## 12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.

Organization personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. In addition, key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. Establish a cyber security organizational structure that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency.

## 13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.

Develop and document a robust information security architecture as part of a process to establish an effective protection strategy. It is essential that organizations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its lifecycle. Of particular importance, an in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure.

## 14. Establish a rigorous, ongoing risk management process.

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management.

# The Basic Form...

Step 1

Step 1

**Identify all connections to SCADA networks.**

**Description**

Action: Conduct a thorough risk analysis to assess the risk and necessity of each connection to the SCADA network. Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected. Identify and evaluate the

**Level 5**

A comprehensive assessment has been made of all connections to the SCADA network. Up-to-date diagrams exist of all connections and there has been a manual inspection of the network to confirm these connections and rule out any undocumented connections. The

**Level 4**

An assessment has been made of all major connections to the SCADA network. Up-to-date diagrams exist for at least 75% of the network. Manual inspections to confirm all undocumented connections have been completed. Work to complete a comprehensive

**Level 3**

An assessment has been made of most major connections to the SCADA network. Up-to-date diagrams exist for at least 50% of the network including manual inspections to confirm undocumented connections. Work to complete a comprehensive assessment is underway.

**Level 2**

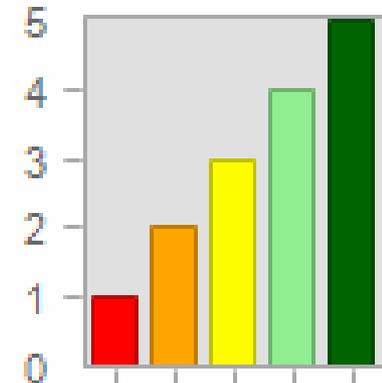
A comprehensive assessment has begun of the connections to the SCADA network. There is now a requirement for systematic manual inspections of all connections to the SCADA network with the goal of documenting the presence of all connections whether authorized or

**Level 1**

A comprehensive assessment has not been made of the connections to the SCADA network. There is no requirement for systematic manual inspections and as a result the presence of unauthorized or undocumented connections cannot be ruled out. There is uncertainty about

Load Levels Save Levels Load Steps Save Steps Security Dashboard >>>

Check a performance level that best captures the security status for this step.



'21 Steps To Improve Cyber Security' Metrics Tool

File Help

Step 21

Establish policies and conduct training for personnel who will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

**Description** Release data related to the SCADA system to persons explicitly authorized to receive it on a strict, need-to-know basis, and only to those persons who have been trained in the proper handling of such information. Social engineering, the gathering of information via questions to naive users, is often the most effective way to obtain sensitive information.

**Level 5** Clear policies have been established to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls. In addition, training and information awareness campaigns are being conducted to ensure that personnel are aware of the risks associated with the inadvertent disclosure of sensitive information.

**Level 4** Clear policies are being established to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls. Training and information awareness campaigns are being planned to ensure that personnel are aware of the risks associated with the inadvertent disclosure of sensitive information.

**Level 3** Some policies have been or are being established to deal with the inadvertent disclosure of sensitive information regarding SCADA system design, operations, or security controls. These policies may include a staff training and information awareness campaign.

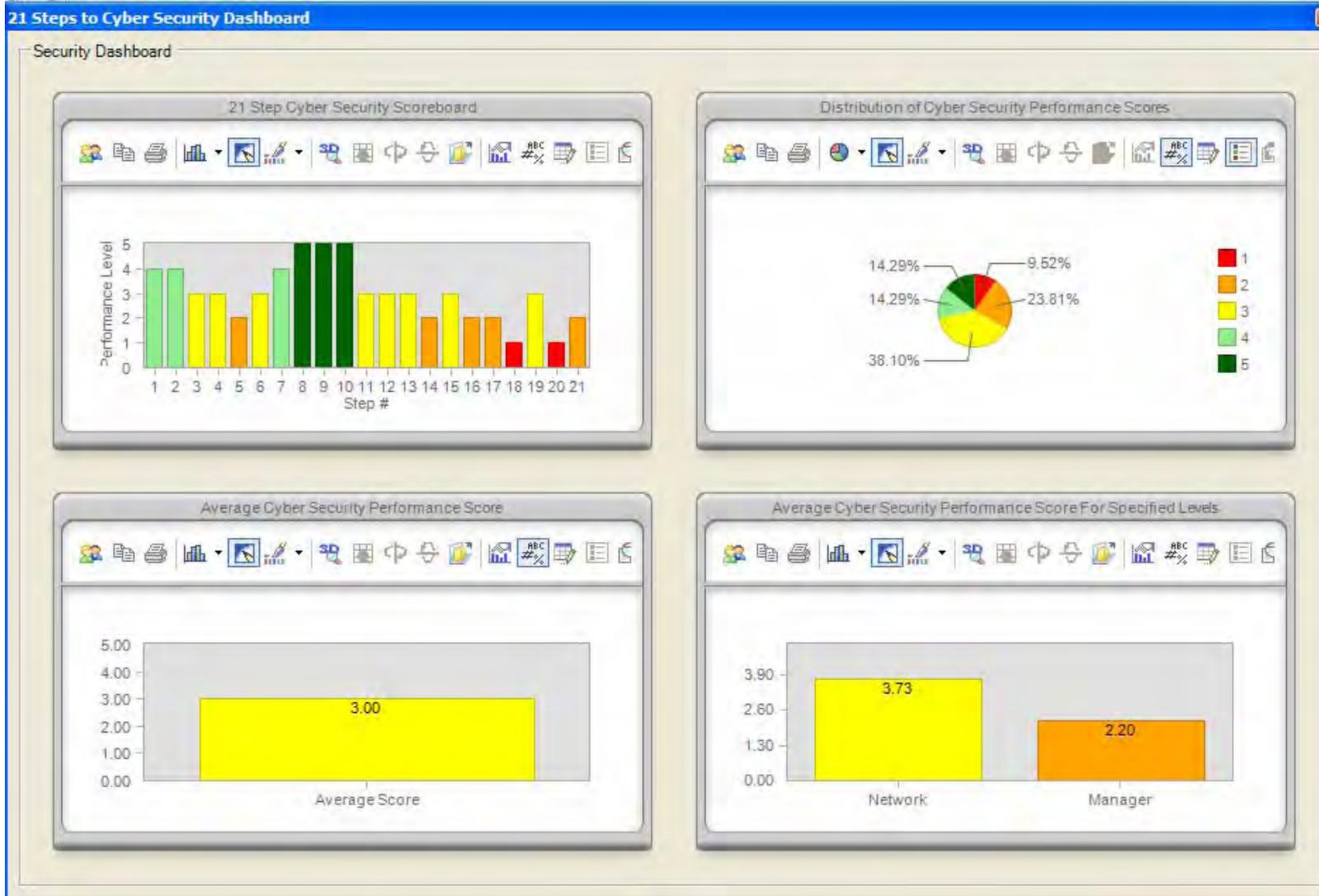
**Level 2** Some policies have been or are being established to deal with the inadvertent disclosure of sensitive information regarding some SCADA system design, operations, or security controls. Staff training and information awareness campaigns are minimal at best.

**Level 1** No policies, staff training, or information awareness campaigns have been established to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding the SCADA system design, operations, or security controls.

Load Levels Save Levels Load Steps Save Steps Security Dashboard >>>>

Complete assessment for each of the 21 steps.

# Dashboard Display

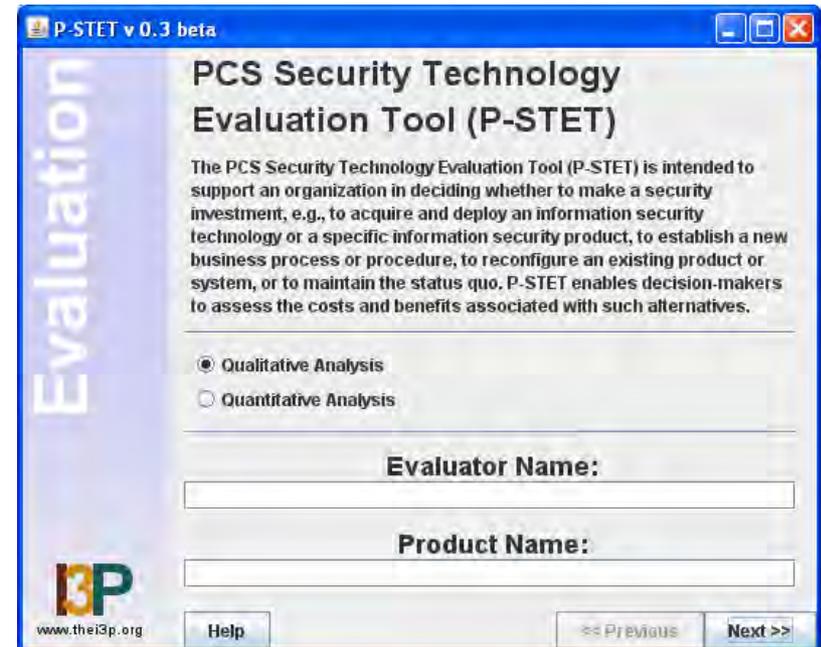


# Explore Options



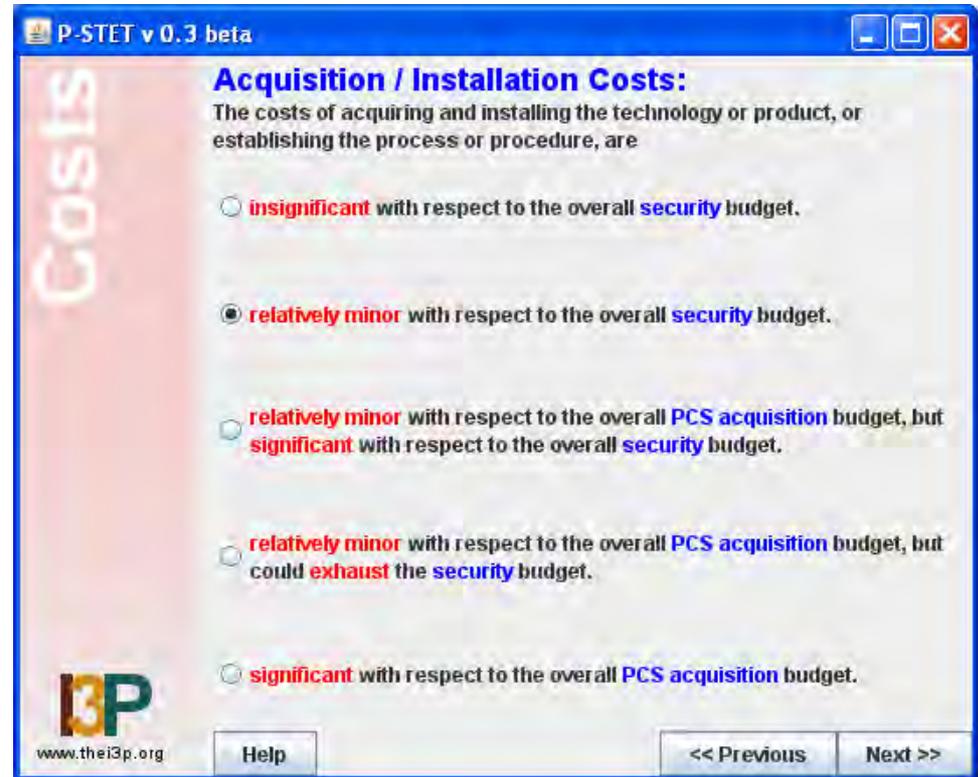
# P-STET

- ◆ P-STET assists in the decision making process from a cost/benefit perspective:
  - How do we acquire and deploy new security technology?
  - How do we reconfigure existing product or system?
- ◆ Qualitative and Quantitative options available
- ◆ Can be tailored to fit an organization's security cost/benefit environment



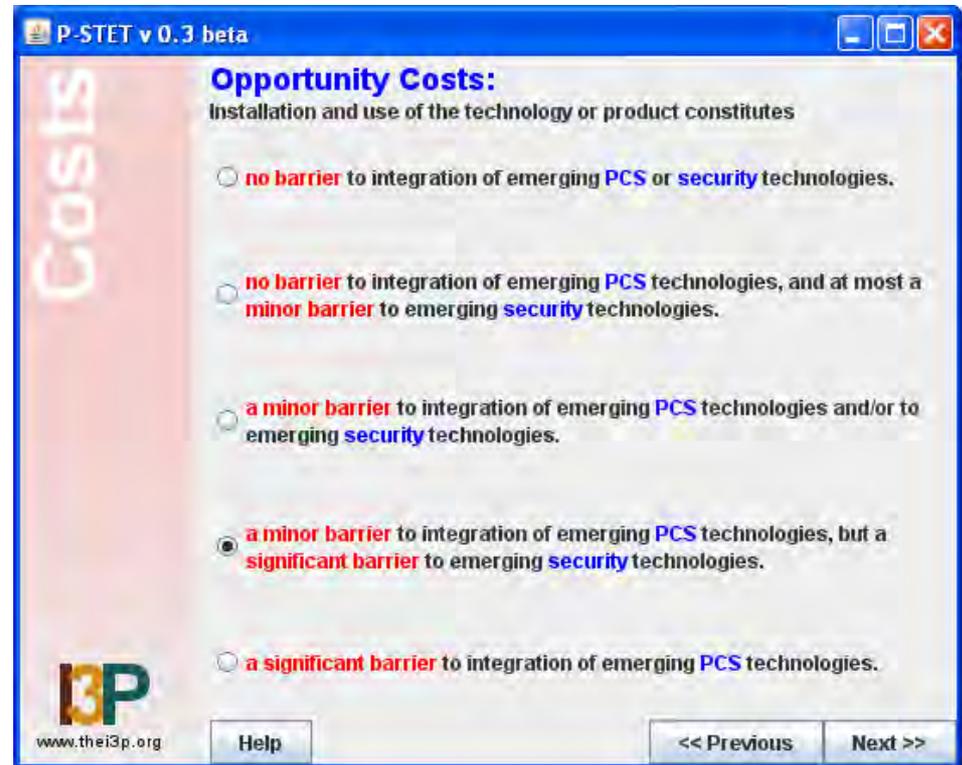
# Qualitative Option: Assessing Costs

- ◆ Acquisition/installation costs
- ◆ Maintenance costs
- ◆ Operations costs -- considers time and resources needed to use the technology



# Qualitative Option: More Costs

- ◆ Operational costs -- impacts on productivity, performance, or latency from using the security technology or product
- ◆ Opportunity costs -- potential problems with interoperability with PCS components or other security technologies.



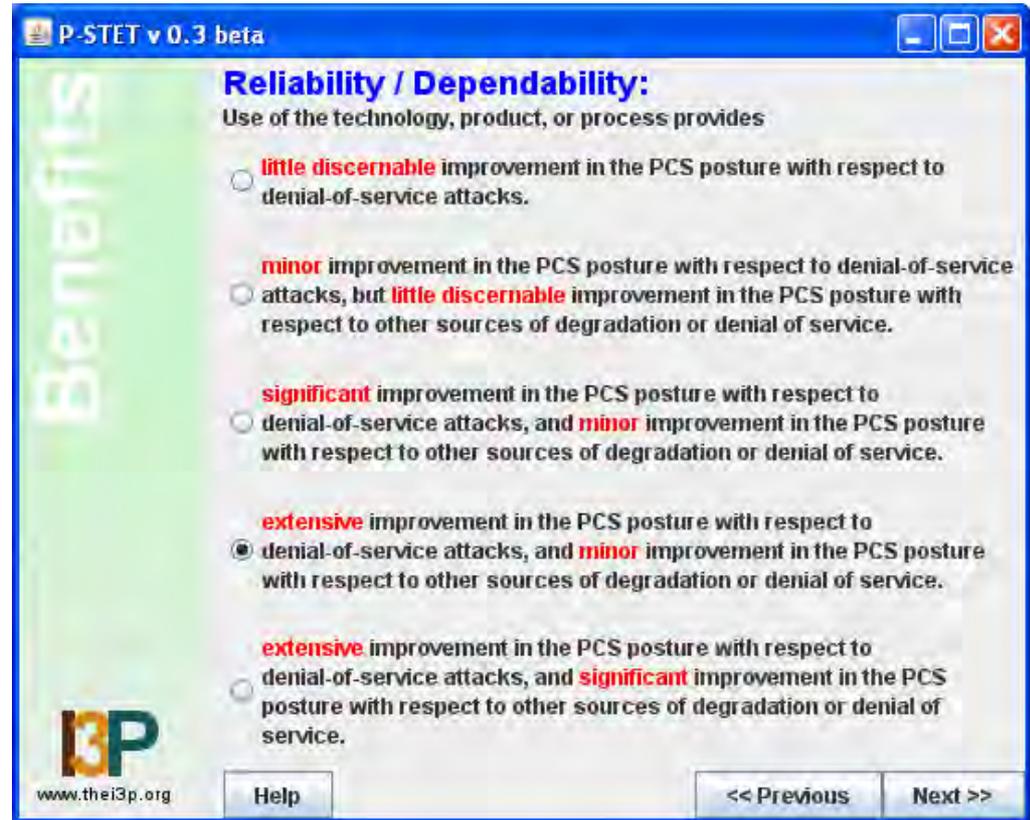
# Qualitative Option: Setting Scales

- ◆ Assigning cost “ranges”, tailored to the organization, such as:
  - Negligible: little or no cost
  - Insignificant: <0.1% of budget
  - Minor:  $\geq 0.1$  to 1% of budget
  - Substantial:  $\geq 1$  to 10% of budget
  - Extensive:  $\geq 10\%$  of budget

*Where “budget” can be the applicable operations or security budget (depending on the application)*

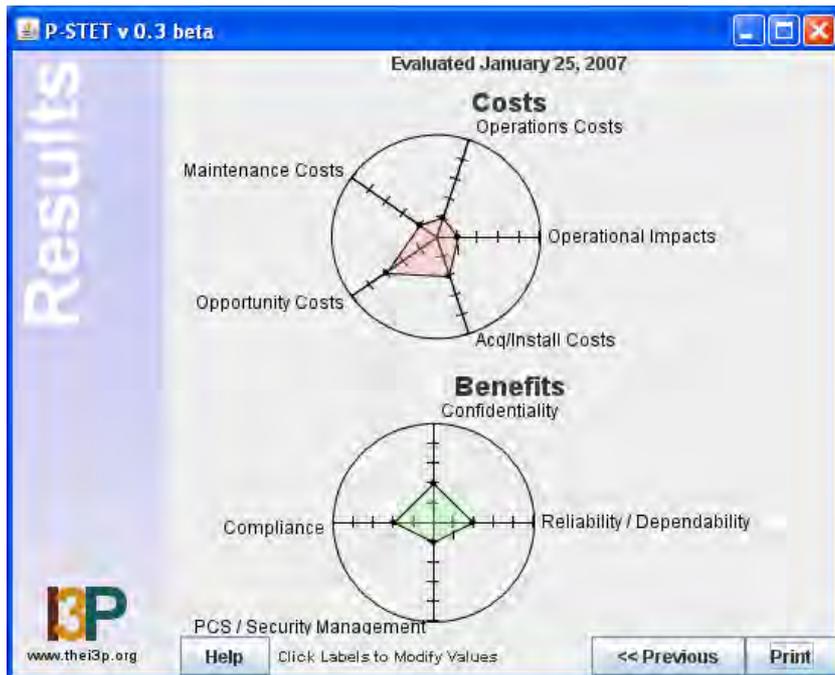
# Qualitative Option: Benefits

- Represented in terms of improvements to operations in the following areas:
  1. Reliability and dependability
  2. Management
  3. Compliance
  4. Confidentiality

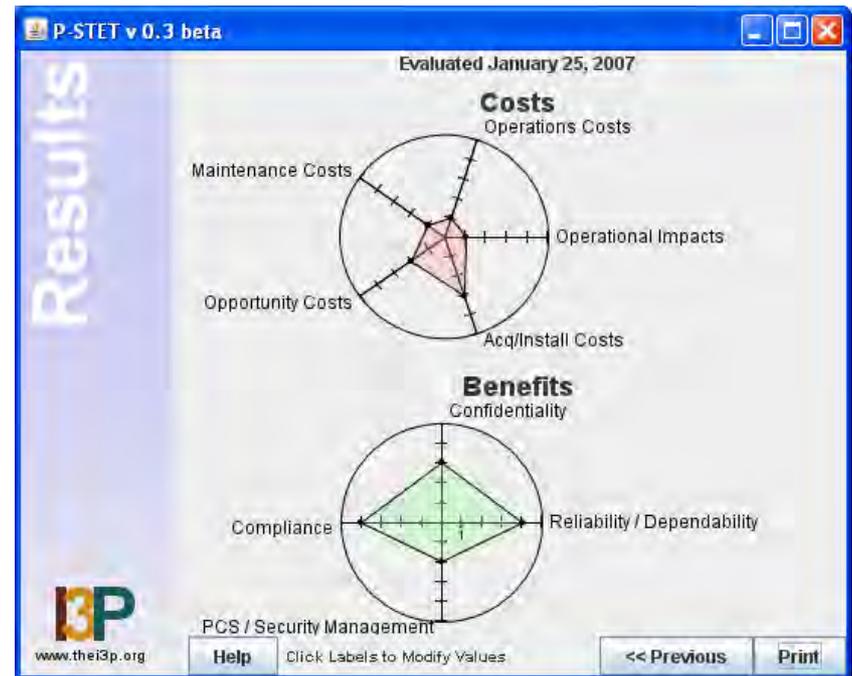


# Qualitative Option: Results

Acceptable



Better!



# Quantitative Option

- ◆ Costs/benefits expressed in terms of dollars
- ◆ Assumes an organization experienced in quantifying things such as cost avoidance
- ◆ P-STET acts as a guide to ensure all cost and benefit angles are viewed

P-STET v 0.3 beta

Evaluated January 25, 2007

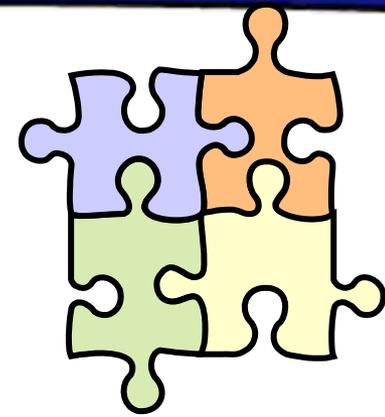
Quantitative

<b>Total Cost of Ownership of Security Product:</b>	
Acquisition/Installation Costs	\$0.00
Maintenance Costs	\$0.00
Operations Costs	\$0.00
<b>Total Cost</b>	<b>\$0.00</b>
<b>Cost Recovery:</b>	
Government Security Grants	\$0.00
Allowable Rate Increases	\$0.00
Other Cost Recovery Methods	\$0.00
<b>Benefits and Cost Avoidance:</b>	
Legal Cost Avoidance (due diligence)	\$0.00
Cyberattack Incident Cost Avoidance	\$0.00
Regulation Compliance Cost Avoidance	\$0.00
Security Enabled Business Advantage	\$0.00
<b>Total Benefit</b>	<b>\$0.00</b>
<b>Total</b>	<b>\$0.00</b>

www.thei3p.org

Print Help Values must be annualized or total for the estimated life of the product

Ok



# Putting the Pieces Together

- ◆ Identify priorities and objectives for security
- ◆ Assess your current security posture with metrics tools
- ◆ Apply security controls and tools in the most critical areas
- ◆ Metrics should be thought of as a tool to achieve your security goals while facilitating your operational objectives.