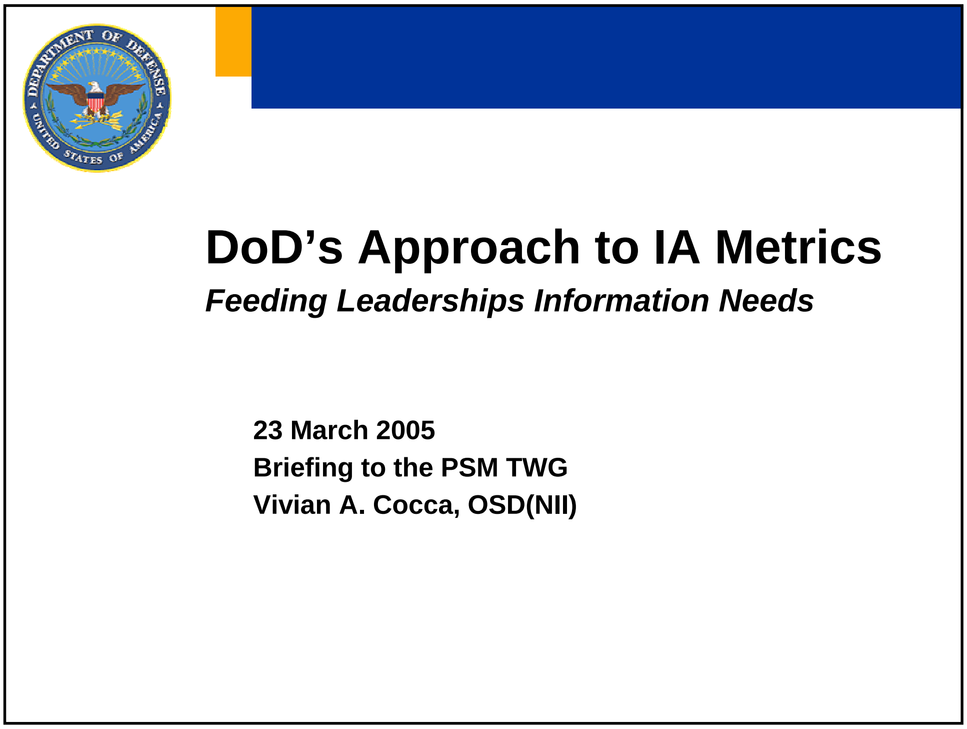
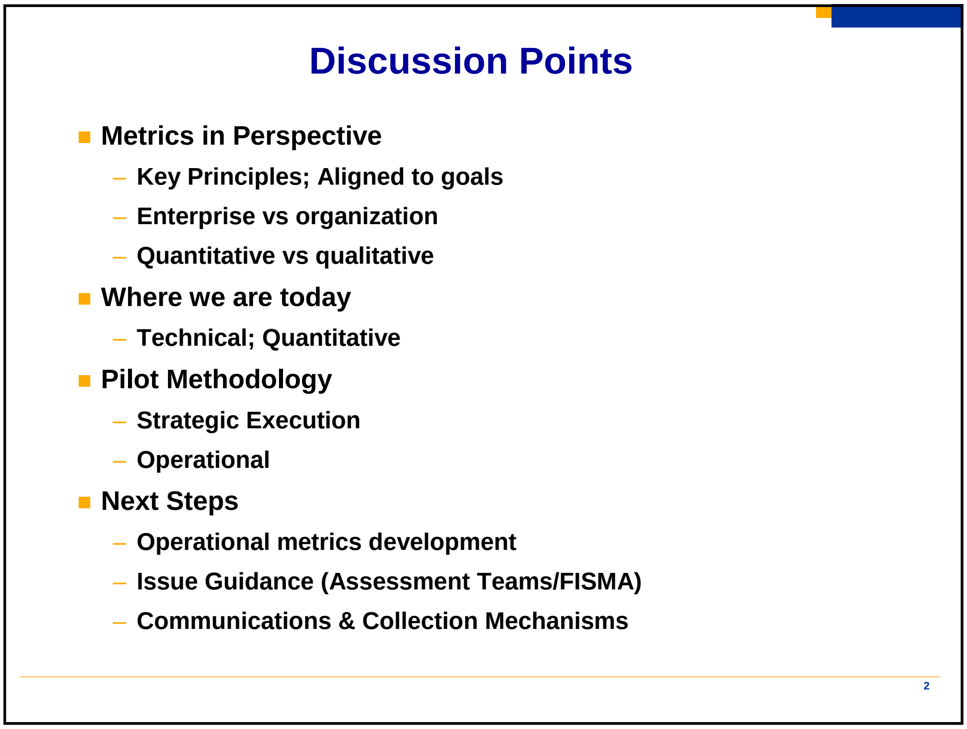


DoD's Approach to IA Metrics

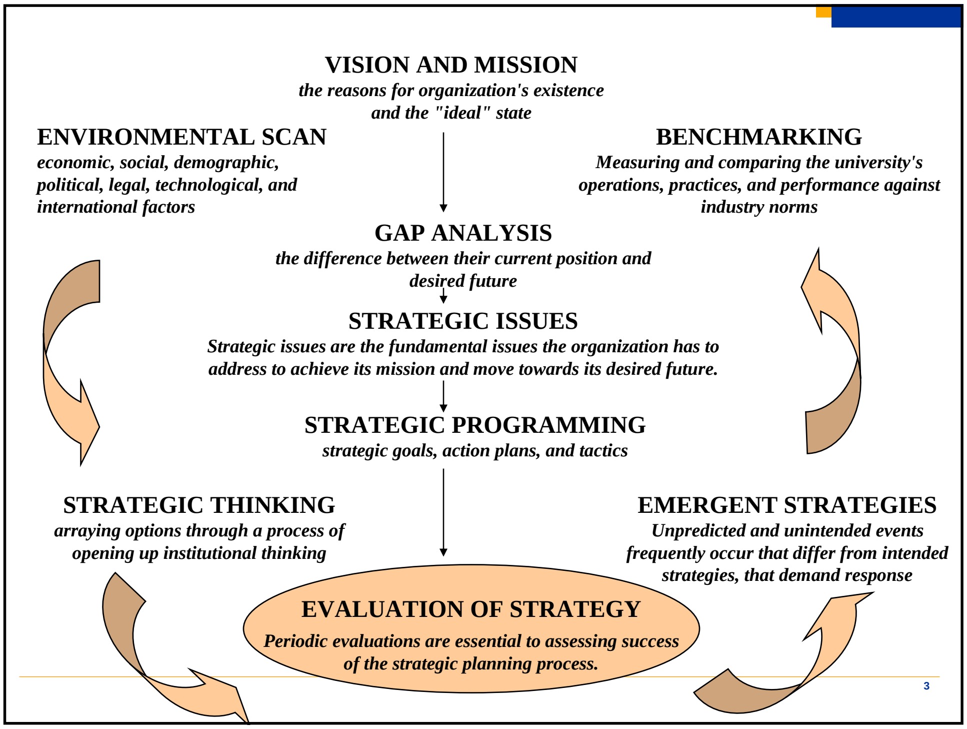
Feeding Leaderships Information Needs

23 March 2005
Briefing to the PSM TWG
Vivian A. Cocca, OSD(NII)



Discussion Points

- Metrics in Perspective
  - Key Principles; Aligned to goals
  - Enterprise vs organization
  - Quantitative vs qualitative
- Where we are today
  - Technical; Quantitative
- Pilot Methodology
  - Strategic Execution
  - Operational
- Next Steps
  - Operational metrics development
  - Issue Guidance (Assessment Teams/FISMA)
  - Communications & Collection Mechanisms



VISION AND MISSION
the reasons for organization's existence and the "ideal" state

ENVIRONMENTAL SCAN
economic, social, demographic, political, legal, technological, and international factors

BENCHMARKING
Measuring and comparing the university's operations, practices, and performance against industry norms

GAP ANALYSIS
the difference between their current position and desired future

STRATEGIC ISSUES
Strategic issues are the fundamental issues the organization has to address to achieve its mission and move towards its desired future.

STRATEGIC PROGRAMMING
strategic goals, action plans, and tactics

STRATEGIC THINKING
arraying options through a process of opening up institutional thinking

EMERGENT STRATEGIES
Unpredicted and unintended events frequently occur that differ from intended strategies, that demand response

EVALUATION OF STRATEGY
Periodic evaluations are essential to assessing success of the strategic planning process.

Vision: Dynamic Information Assurance for the GIG

Mission: Assure DoD's Information, Information Systems, Information Infrastructure and support the Departments Transformation to Network and Data-Centric Operations and Warfare

Core Competencies

<u>Goal #1 – Protect Information</u>

(Secure, Verifiable, Available)

<u>Goal #2 – Defend Systems & Networks</u>

(Resist, Recognize, React, Recover, Reconstitute)

<u>Goal #3 – Situational Awareness/C2</u>

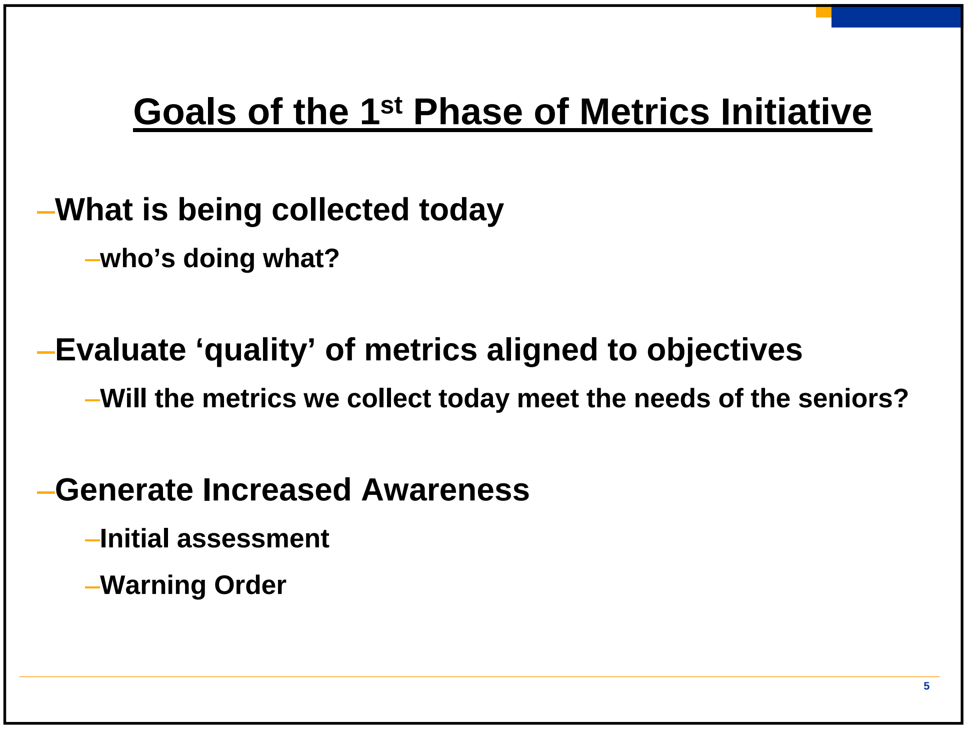
(Shared awareness, Synchronized response, C2)

<u>Goal #4 – Transform & Enable IA Capabilities</u>

(Adaptation, Visibility & Alignment, Innovation & Agility)

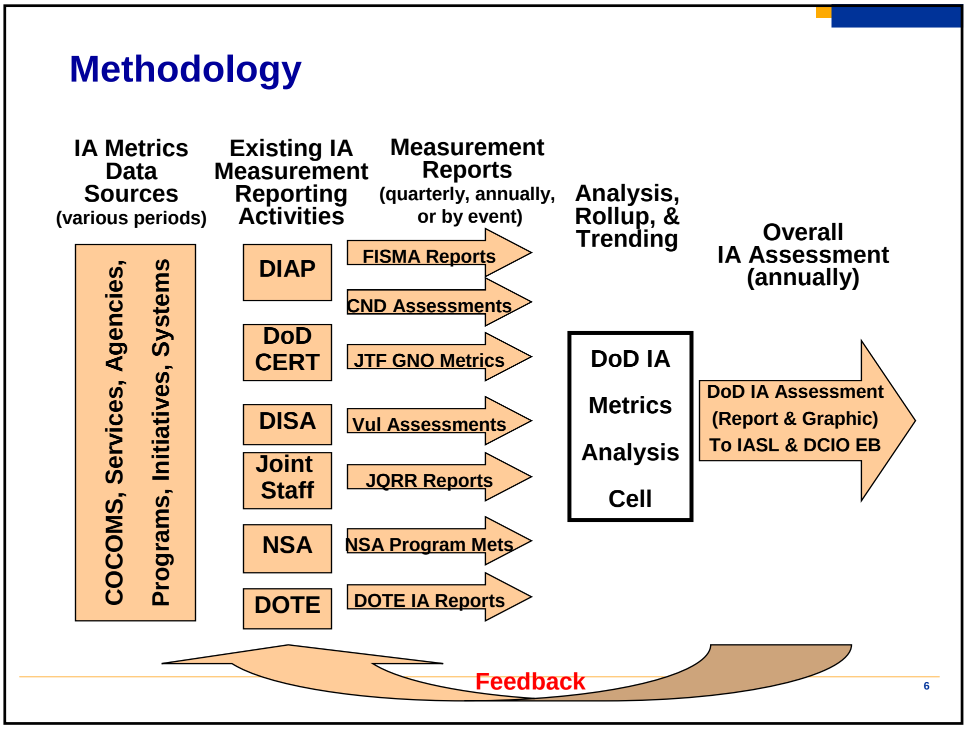
<u>Goal #5 – Create an IA Empowered Workforce</u>

(Identification, Alignment, Competency Development & Maintenance, Resource Availability)



Goals of the 1st Phase of Metrics Initiative

- What is being collected today
  - who's doing what?
- Evaluate 'quality' of metrics aligned to objectives
  - Will the metrics we collect today meet the needs of the seniors?
- Generate Increased Awareness
  - Initial assessment
  - Warning Order



Methodology

IA Metrics Data Sources (various periods)

Existing IA Measurement Reporting Activities

Measurement Reports (quarterly, annually, or by event)

Analysis, Rollup, & Trending

Overall IA Assessment (annually)

COCOMS, Services, Agencies, Programs, Initiatives, Systems

DIAP

DoD CERT

DISA

Joint Staff

NSA

DOTE

FISMA Reports

CND Assessments

JTF GNO Metrics

Vul Assessments

JQRR Reports

NSA Program Mets

DOTE IA Reports

DoD IA Metrics Analysis Cell

DoD IA Assessment (Report & Graphic) To IASL & DCIO EB

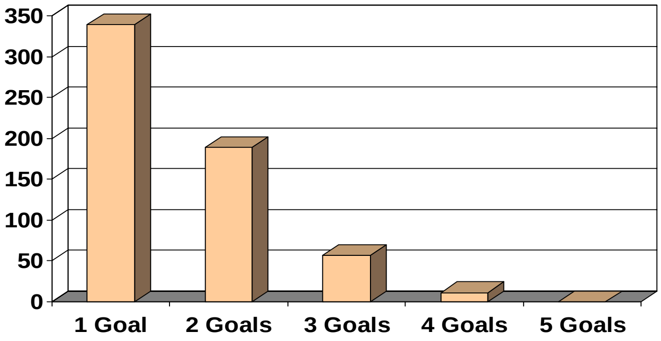
Feedback

IA Metrics Working Group Results

- Collected, Documented, Categorized over 700 metrics from existing metrics efforts across the DoD
  - JTF-GNO, DISA, NSA, JQRR, & DOTE metrics
  - FISMA and CND Assessments
- Analyzed the knowledge needs for assessing each goal area of the strategic plan
- Analyzed the existing metrics from two perspectives:
  - Which ones supported our knowledge needs to assess our progress towards our goals
  - What is the quality of each metric… based on solid data? or more subjective?
- Aligned & assessed if adequate for our needs
- Here is what we discovered:
  - Over 200 existing metrics weren’t ‘good metrics’ for our purposes
  - We have a lot of gaps in our current knowledge base

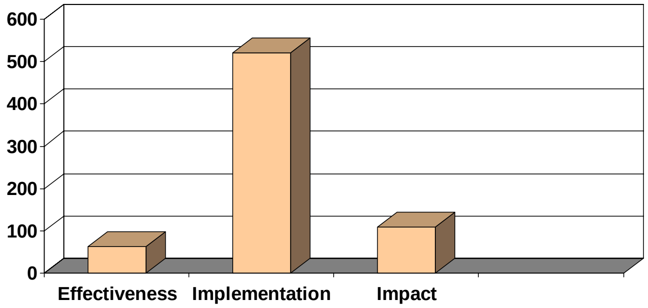
Metrics Overlap Across IA Goals

- Over half of existing metrics apply to only one IA Goal
- Only ~10% of existing metrics apply to more than two IA Goals
  - Should result in reasonably clean relationship between changes in metrics and progress towards reaching Goal



Effectiveness versus Implementation Metrics

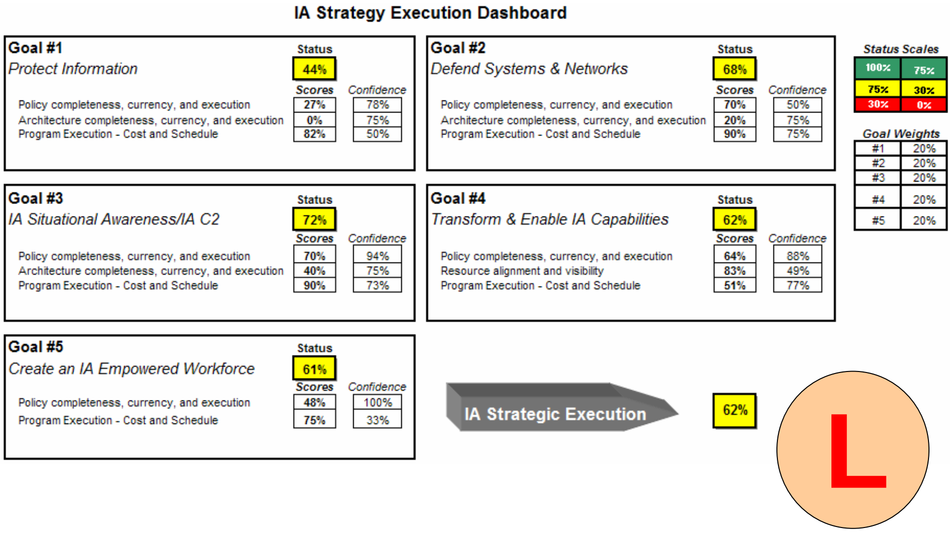
- Most existing metrics are implementation metrics
- Candidate metrics sources to consider for increasing number of effectiveness metrics:
  - Incident metrics from JTF GNO
  - Red team result metrics
  - Vulnerability assessment results



Some Insights…

- DoD is really good at implementation metrics; not so good at outcome & really not good at linkages
- Senior leadership does not spend enough time identifying what is important to mission success or does not communicate it effectively to providers
  - Need to identify what is important to them
  - Need repeatable ways to communicate & track
  - Need dedicated investment in management of the process
- Bottom up→quantitative, standards driven, tool based implementation of collection mechanisms
- Top down→qualitative, simplified, yet tied to ‘real data’
- Do not have a good understanding of risk & no good way to frame investment decisions in terms of risk to mission, function, forces
- Really complicated; not enough time spent on analysis

Results (preliminary) – Enterprise Summary



IA Strategy Execution Dashboard

Goal #1
Protect Information
Status: 44%

	Scores	Confidence
Policy completeness, currency, and execution	27%	78%
Architecture completeness, currency, and execution	0%	75%
Program Execution - Cost and Schedule	82%	50%

Goal #2
Defend Systems & Networks
Status: 68%

	Scores	Confidence
Policy completeness, currency, and execution	70%	50%
Architecture completeness, currency, and execution	20%	75%
Program Execution - Cost and Schedule	90%	75%

Goal #3
IA Situational Awareness/IA C2
Status: 72%

	Scores	Confidence
Policy completeness, currency, and execution	70%	94%
Architecture completeness, currency, and execution	40%	75%
Program Execution - Cost and Schedule	90%	73%

Goal #4
Transform & Enable IA Capabilities
Status: 62%

	Scores	Confidence
Policy completeness, currency, and execution	64%	88%
Resource alignment and visibility	83%	49%
Program Execution - Cost and Schedule	51%	77%

Goal #5
Create an IA Empowered Workforce
Status: 61%

	Scores	Confidence
Policy completeness, currency, and execution	48%	100%
Program Execution - Cost and Schedule	75%	33%

Status Scales

🟩 100%	🟩 75%
🟨 75%	🟨 30%
🟥 30%	🟥 0%

Goal Weights

#1	20%
#2	20%
#3	20%
#4	20%
#5	20%

IA Strategic Execution 62%

L

DoD IA Program – Leadership Responsibilities

"Operate today, plan for tomorrow,
invest for the future & guide the transformation"

-Minimize Risk to Mission-

Requires:

1. **Understanding of the operational environment *(operations)***

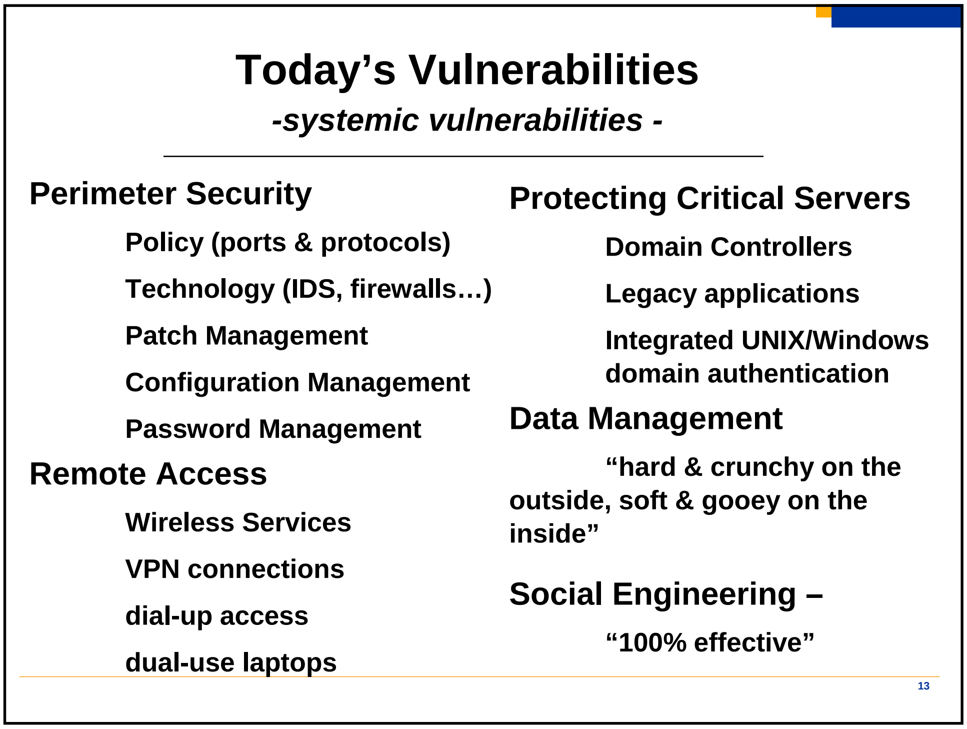
   -what should I invest in <u>now</u> to mitigate risk to operations?

2. **Knowledge of gaps between as-is and to-be *(strategy)***

   -what investments do I need to make for <u>tomorrow</u>?

3. **Assumed Risk (today vs. tomorrow) *(risk mitigation)***

   -what are the tradeoffs in terms of <u>risk to mission</u>?



Today’s Vulnerabilities

-systemic vulnerabilities -

Perimeter Security

- Policy (ports & protocols)
- Technology (IDS, firewalls…)
- Patch Management
- Configuration Management
- Password Management

Remote Access

- Wireless Services
- VPN connections
- dial-up access
- dual-use laptops

Protecting Critical Servers

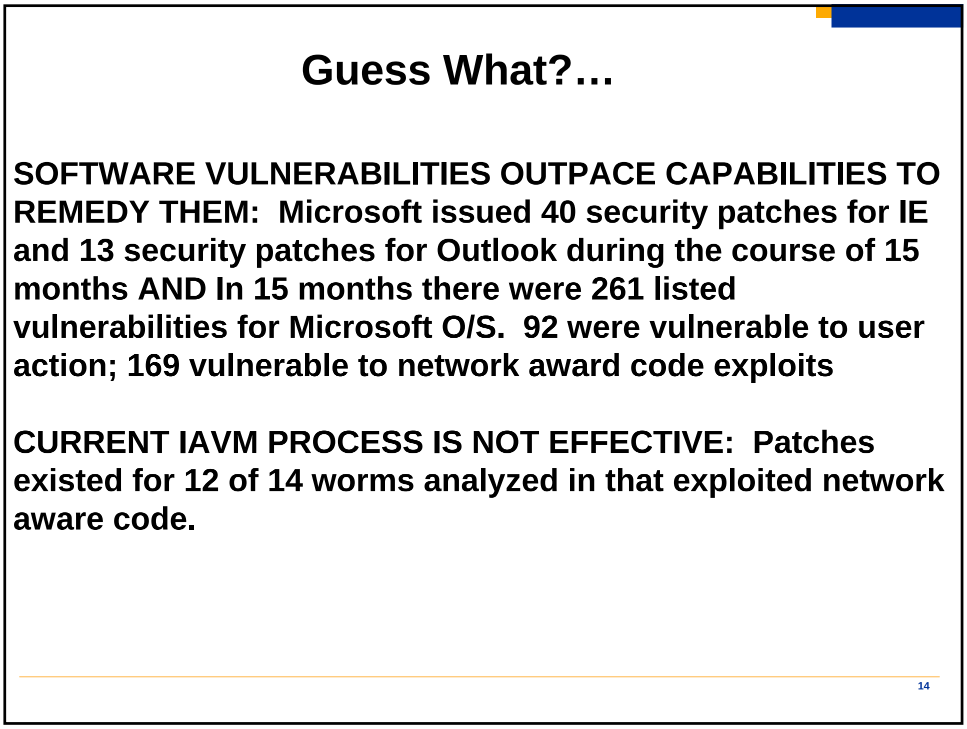
- Domain Controllers
- Legacy applications
- Integrated UNIX/Windows domain authentication

Data Management

“hard & crunchy on the outside, soft & gooey on the inside”

Social Engineering –

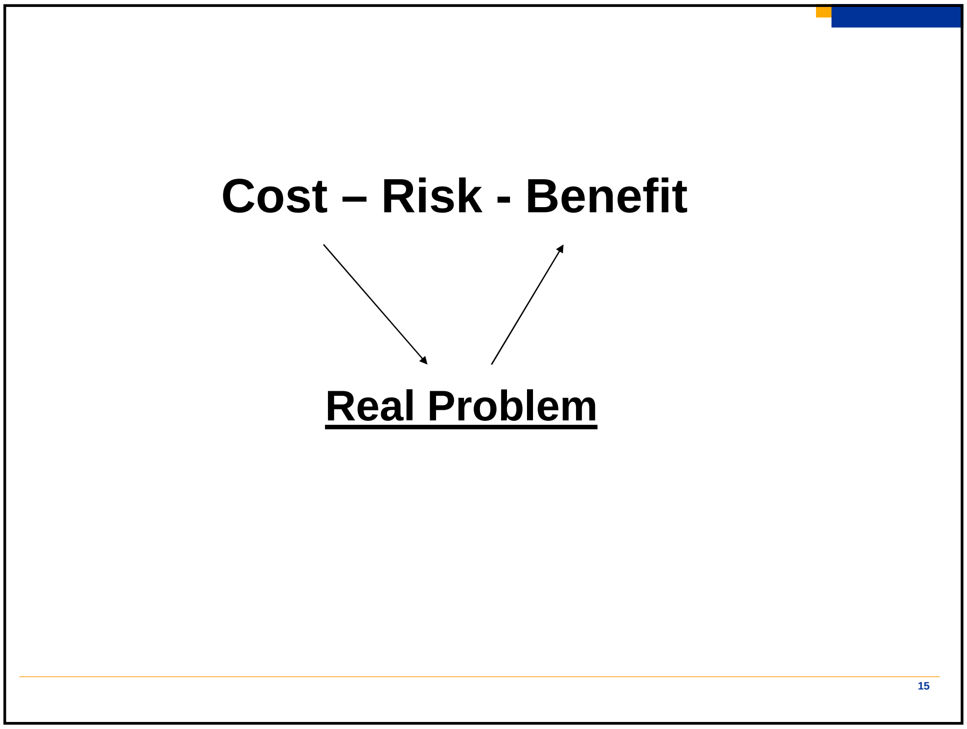
“100% effective”



Guess What?…

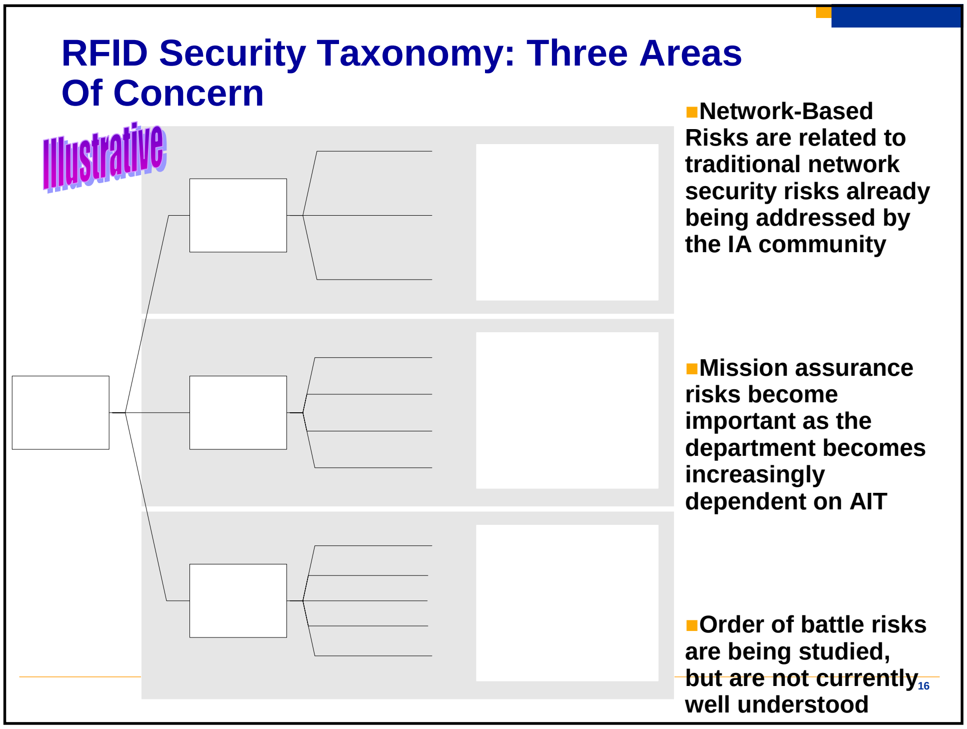
SOFTWARE VULNERABILITIES OUTPACE CAPABILITIES TO REMEDY THEM: Microsoft issued 40 security patches for IE and 13 security patches for Outlook during the course of 15 months AND In 15 months there were 261 listed vulnerabilities for Microsoft O/S. 92 were vulnerable to user action; 169 vulnerable to network award code exploits

CURRENT IAVM PROCESS IS NOT EFFECTIVE: Patches existed for 12 of 14 worms analyzed in that exploited network aware code.



Cost – Risk - Benefit

Real Problem



RFID Security Taxonomy: Three Areas Of Concern

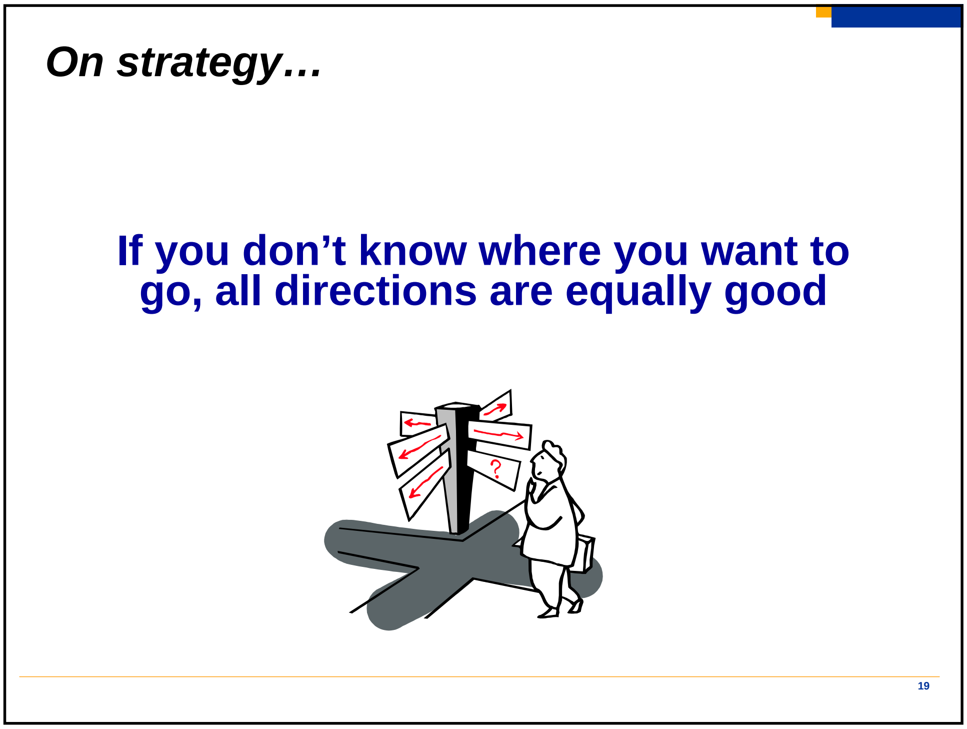
- Network-Based Risks are related to traditional network security risks already being addressed by the IA community
- Mission assurance risks become important as the department becomes increasingly dependent on AIT
- Order of battle risks are being studied, but are not currently well understood

Core Principles for a Successful Executive-Level Metrics Program

- Measures of progress (metrics) must be tied to specific goals that are important to management.
- Staff should understand the importance of the goals and the role of the metrics in accomplishing them- help them to become excited about the metrics.
- Executive-level metrics should be understandable to management.
- Metrics are indicators that the goals are being achieved - they are not themselves the goals.
- It’s important to find good metrics - bad metrics can impede progress towards the goals (outcome & goal focused)
- Metrics will likely change as progress is made towards the goals.
- Tracking metrics requires gathering and analyzing data periodically (quarterly) - establish efficient mechanisms to do this.
- Different parts of organizations will require varying levels of detail - try to establish executive level metrics that are rollups or extracts from lower level metrics. Lower level organizations should own the metrics at their level.

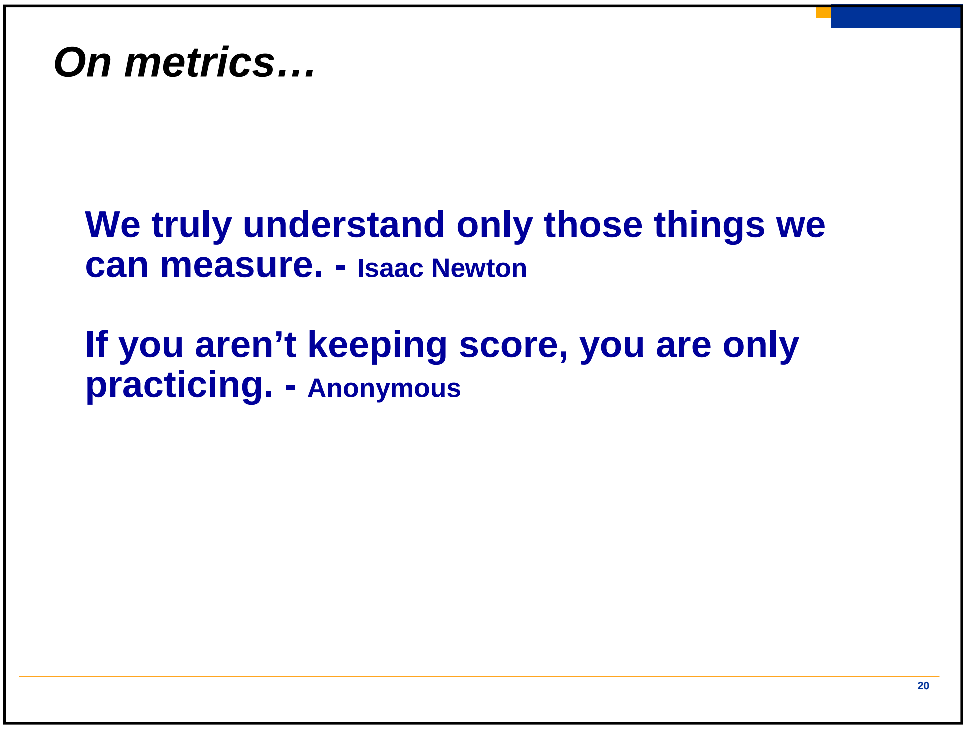
K I S S

Keep it Simple, Staff!



On strategy…

If you don't know where you want to go, all directions are equally good



On metrics…

We truly understand only those things we can measure. - Isaac Newton

If you aren't keeping score, you are only practicing. - Anonymous