Toward Performance-Based IT Security at NASA: A Journey

Presented to

Computer system Security and Privacy Advisory Board

March 7, 2002

Dr. David B. Nelson, CISSP
NASA Deputy CIO
dnelson@hq.nasa.gov

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

NASA Situation Analysis

- NASA primarily a research organization with many ties to academic and international partners and statutory responsibility for public communication and education; but some operations highly sensitive or critical
  - **Security with openness; pockets of tight security**
- Very decentralized IT — most operational responsibility at ten field Centers with staff who do not blindly follow orders
  - **Security by consensus; Agency-level leadership with insight via metrics**
- Trend towards more centralized IT management to support enterprise-wide functions
  - **Enhance security while managing change**

Evolution of Current NASA IT Security

- 1998-99 Internal Review of NASA IT Security
  - 33 recommendations accepted by Administrator for implementation in areas of policy, procedures, staff, technology
- 1999 GAO Audit
  - Confirmed internal study and added urgancy
- 1998-2002 Numerous IG audits
  - Added detail and kept spotlight on progress
- 2001 Government Information Security Act Report
  - NASA C- grade by Horn Committee (average F)
  - Conditional approval of NASA ITS by OMB

NASA ITS Management Philosophy

- IT Security is part of mission accomplishment
  - Most ITS responsibility and actions are owned by program/project management
  - CIO provides overall leadership and oversight
  - Some agency-wide activities centrally managed, but closely coordinated with program management
- NASA practices ITS risk management, not risk avoidance
  - Risks are assessed, understood, and mitigated to level acceptable to management
  - Information and functions of differing criticality are protected at different levels

Goals are derived from Management Philosophy and Current Situation

- NASA and contractor employees understand IT security responsibilities and demonstrate skills needed to carry them out.
- System and application vulnerabilities are kept at a level where operations are not jeopardized.
- NASA, collectively, is alert to intrusion attempts and takes effective action to thwart them.
- NASA utilizes an effective infrastructure for authentication, access control, digital signature, and encryption.
- NASA maintains effective policies and guidance for IT security, based on law, regulation, best practices, and NASA's particular needs.

Why Measure Progress?

- We truly understand only those things we can measure. - Isaac Newton
- If you aren't keeping score, you are only practicing. - Anonymous

Measuring Progress(1)

- Measures of progress (metrics) must be tied to specific goals that are important to management.
- 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.
- Metrics will likely change as progress is made towards the goals.

Measuring Progress(2)

- 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.
- 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.

NASA Process for Establishing and Tracking Yearly Metrics

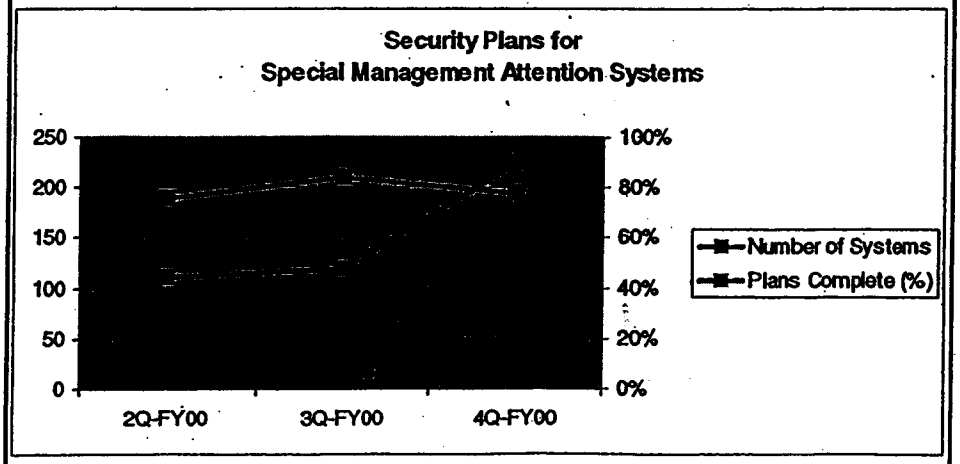
- February-March: small group drafts proposed metrics based on goals and past year experience
- April: ITS Managers debate and adopt metrics
- June: CIO's debate and adopt metrics
- August: NASA Security Council endorses metrics
- September: NASA CIO issues memo transmitting adopted metrics for next fiscal year
- January, April, July, October: progress of metrics collected, discussed with management, needed action taken

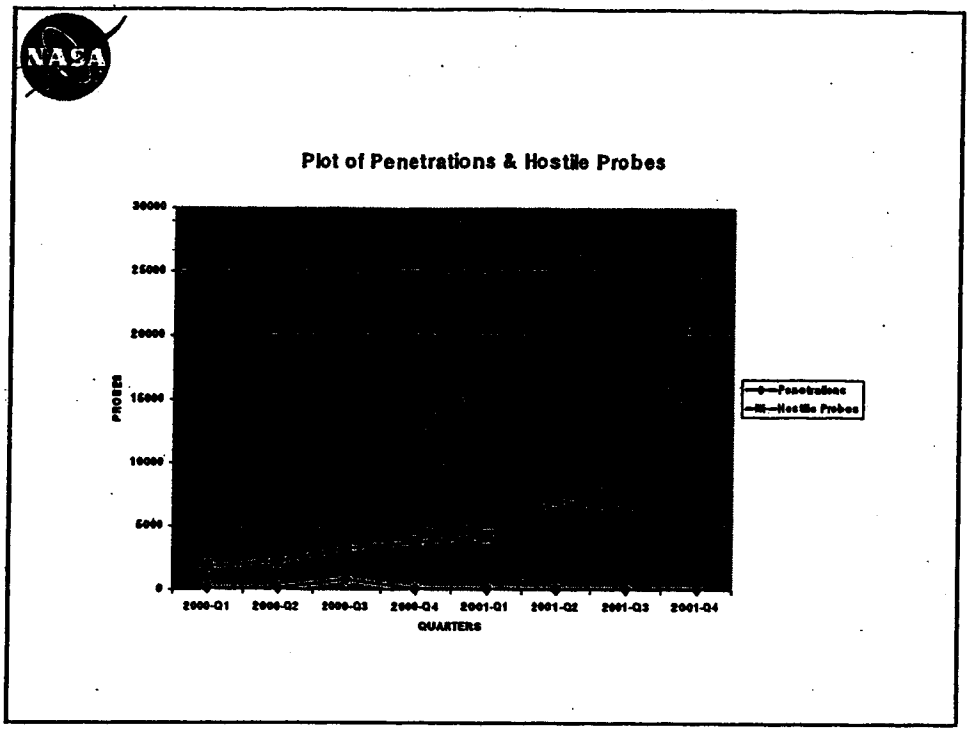
Examples of FY2002 IT Security Metrics

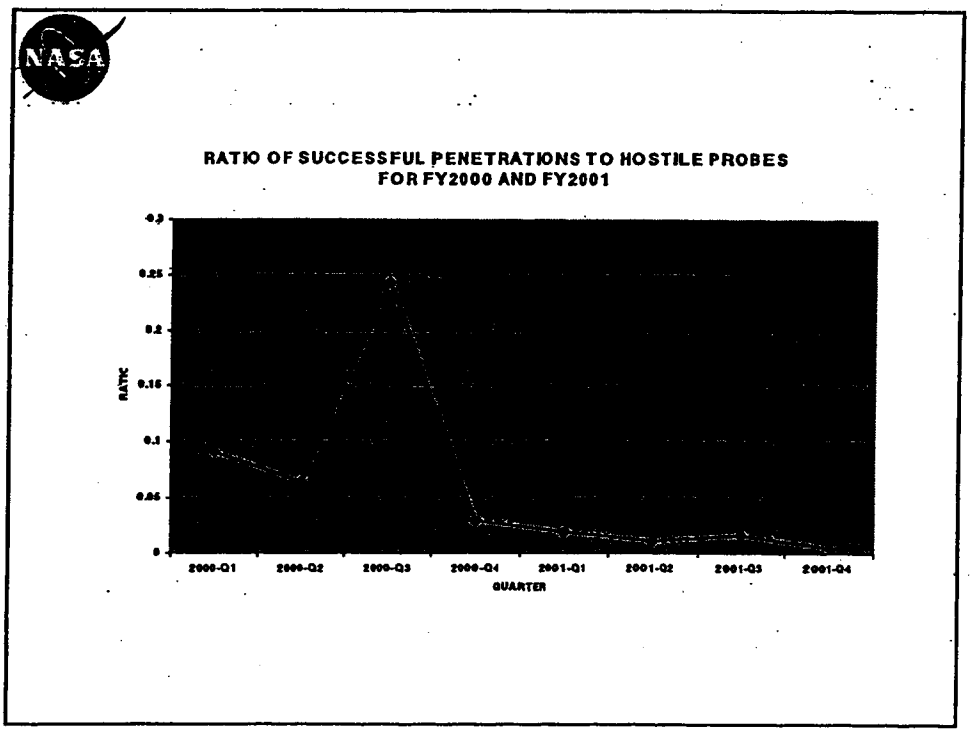
Goal 1: NASA and contractor employees understand ITS responsibilities and demonstrate skills needed to carry them out.

- **A. Employees' General Awareness (civil service, JPL Cal Tech, and contractors)**
  - **By July 1, 2002– 90 percent will have successfully completed the "Basic ITS Awareness for 2002" training on SOLAR or equivalent training. (This metric is reportable to Congress under GPRA.)**
- **B. NASA Managers (civil service and JPL Cal Tech)**
  - **By July 1, 2002 – 95 percent will have successfully completed the "Basic ITS Awareness for 2002 with Managers' Supplement" training on SOLAR or equivalent training (This metric is reportable to Congress under GPRA.)**
- **C. Line Managers Authorizing SMA, MSN, or BRT Systems**
  - **By July 1, 2002 – 95 percent will have successfully completed the "Basic ITS Awareness for 2002 with Managers' Supplement" training on SOLAR or equivalent training (This metric is reportable to Congress under GPRA.)**
  - **By July 1, 2002 – 90 percent will have successfully completed the "Managers Responsibilities for ITS Risk Management" training on SOLAR or equivalent training. Training must have occurred within the last 3 years.**

Measuring Progress Focuses Attention




Plot of Penetrations & Hostile Probes
PROBES
QUARTERS
2000-Q1
2000-Q2
2000-Q3
2000-Q4
2001-Q1
2001-Q2
2001-Q3
2001-Q4
Penetrations
Hostile Probes


RATIO OF SUCCESSFUL PENETRATIONS TO HOSTILE PROBES
FOR FY2000 AND FY2001
RATIO
QUARTER
2000-Q1
2000-Q2
2000-Q3
2000-Q4
2001-Q1
2001-Q2
2001-Q3
2001-Q4

What's Next?

- NASA is approaching "competence" after three years of hard work
  - policies, plans, staff, training, technology, metrics, response, follow-up in place (more or less)
  - appropriate budget of 5% of IT budget
  - but too reactive and too much manual labor
  - not enough integration into program management
- Next three years will be striving for "excellence"
  - being smarter, not spending more money
  - better intelligence through better data and analysis
  - better and more automated processes
  - reduce duplication through Agency-level processes
  - better integration into program and capital planning

Resources

- GAO Special Publications (http://www.gao.gov)
  - "Measuring Performance and Demonstrating Results of Information Technology Investments"
  - "Information Security Management: Learning From Leading Organizations"
  - "Information Security Risk Assessment: Practices of Leading Organizations"
- SANS Institute
  - http://www.sans.org
- NIST
  - http://csrc.nist.gov/
- NASA IT Security Directives NPD 2810, NPG 2810
  - http://nodis.hq.nasa.gov/Library/Directives/NASA-WIDE/Procedures/Legal_Policies/contents.html