

**JPL's Infrastructure for Managing IT Security:
The Processes and Custom Toolset**

**Robert L. Miller, Ph.D.
JPL IT Security Implementation Manager**

April 23, 2003

Agenda

What problem are we trying to solve?

How did we solve it?

- Processes
- Tools
- Metrics
- Follow Up

Demonstrations

- IT Security Database (ITSDB)
- Security Problem Log (SPL)
- IT Status Reporting (ITSR)

What Problem Are We Trying To Solve?

Change JPL's IT culture to internalize the need for (and cost of) improving IT security

Develop and maintain meaningful and auditable security plans

- Snapshots quickly become inaccurate
 - IT assets arrive, leave, and move daily
 - People arrive, leave, and move daily
 - Organizations change periodically
- Paper plans cannot be easily queried
- Paper plans do not readily support external audits

What Problem Are We Trying To Solve?

Aggressively manage security vulnerabilities, from detection through verified correction

- Quick, secure communication of problem description, corrective action, and deadline for fixing to accountable system administrator (SA)
- Automatic escalation to line manager when correction is overdue

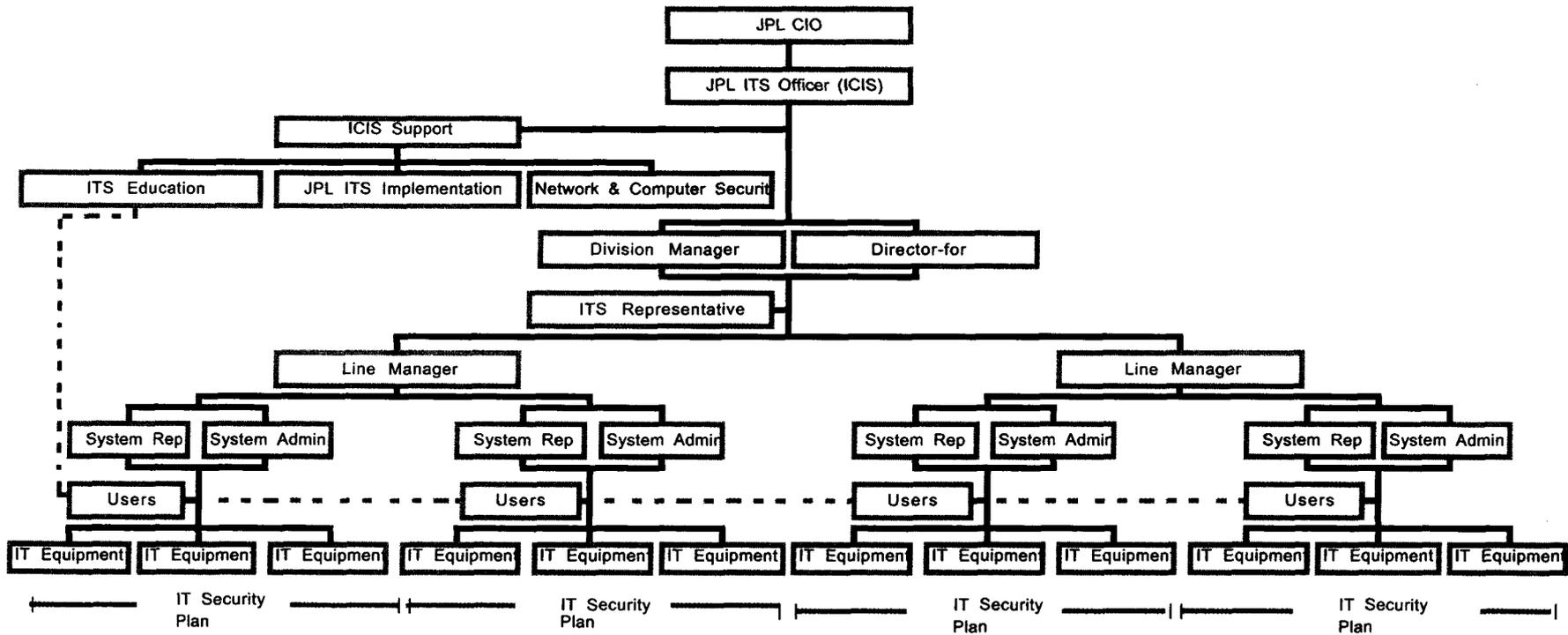
Maintain JPL IT Contingency Plan (ITCP) for critical operational Projects and Programs

- Develop a local ITCP as part of each IT Security Plan

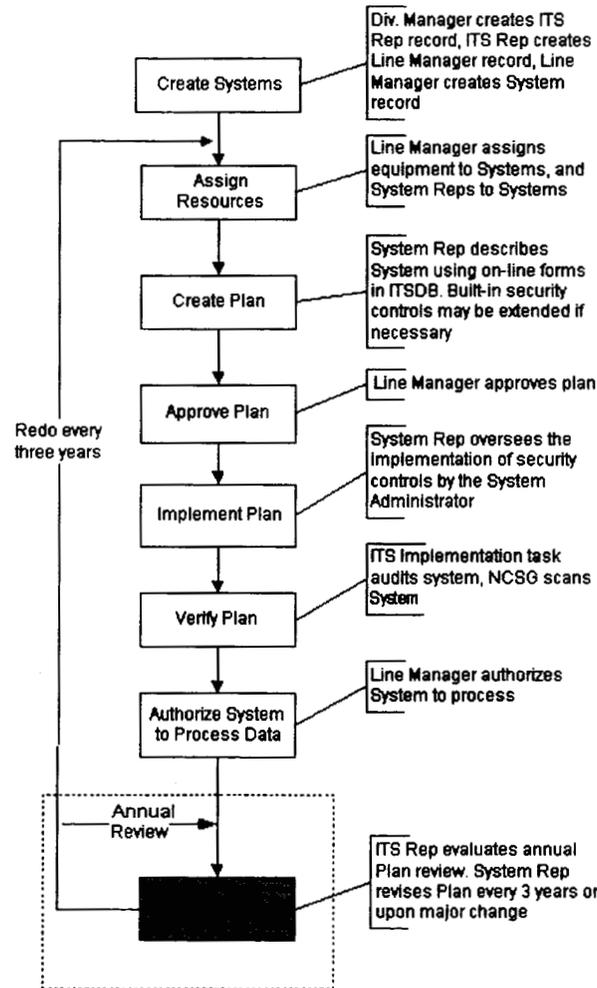
How Did We Solve It?

- 1. Analyzed NPG 2810**
- 2. Designed a detailed security planning process that traced each step to NPG 2810**
- 3. Identified roles and responsibilities (pages 6, 7)**
- 4. Obtained senior management's approval to proceed and assign IT Security Representatives (like CSO)**

IT Security Responsibility and Planning Roles



JPL IT Security Planning Process Overview



How Did We Solve It?

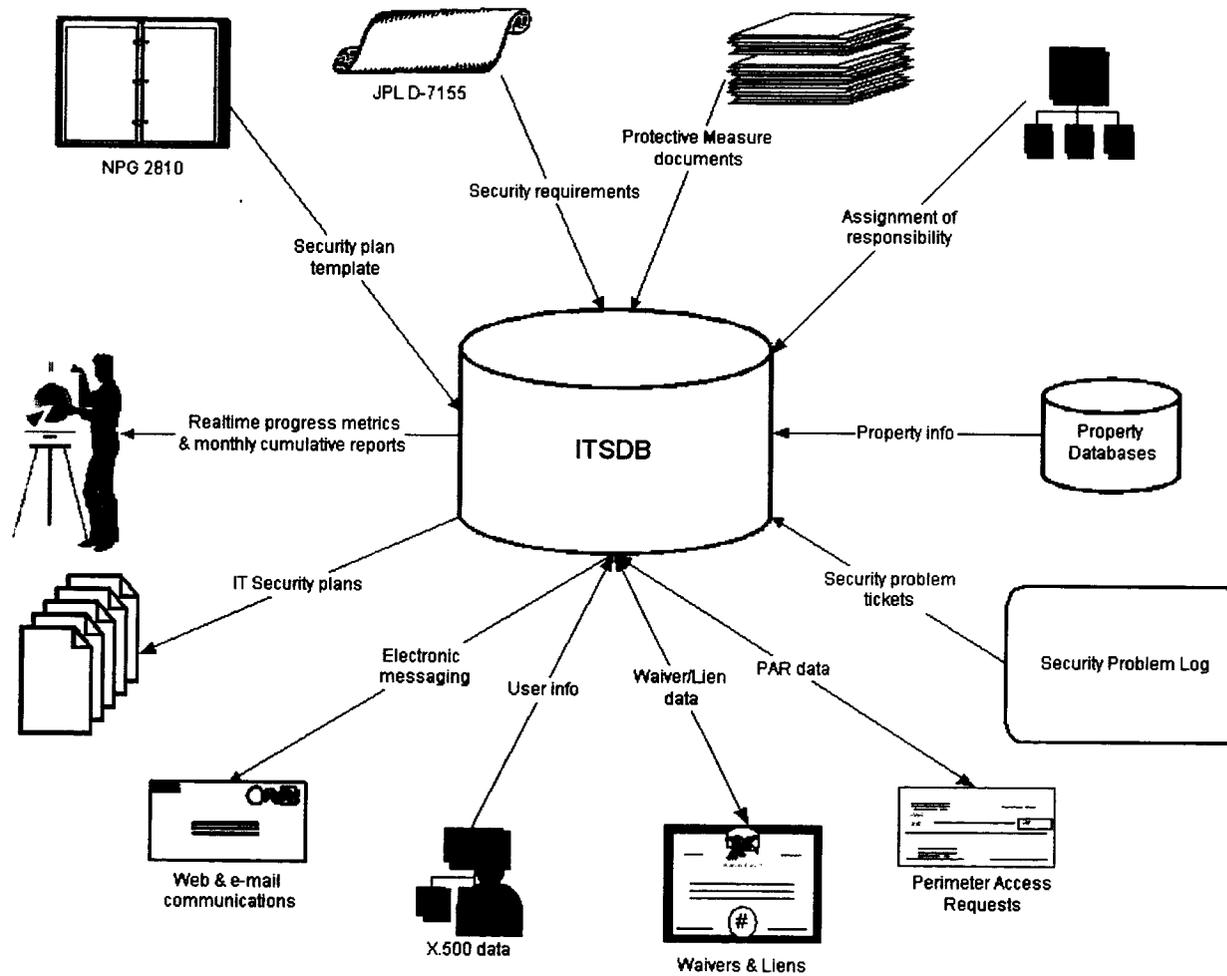
- 5. Provided training and consulting to build support**
- 6. Engineered an understandable and efficient process to achieve compliance across JPL**
 - Created common tools, templates, and databases
 - Usable by Mac, PC, and Unix communities
 - Only ask for required, local information
 - Automate database maintenance where possible
 - Assignment of assets to organizations
 - Asset location and IP address
 - Listened to the users
 - Problems due to software limitations or lack of training
 - Wish list items
 - Fast response to questions and complaints
 - Developed real-time implementation status metrics
 - Implementers and management see progress toward scheduled goals
 - Identify stragglers or bottlenecks for timely attention or remediation

IT Security Database (ITSDB)

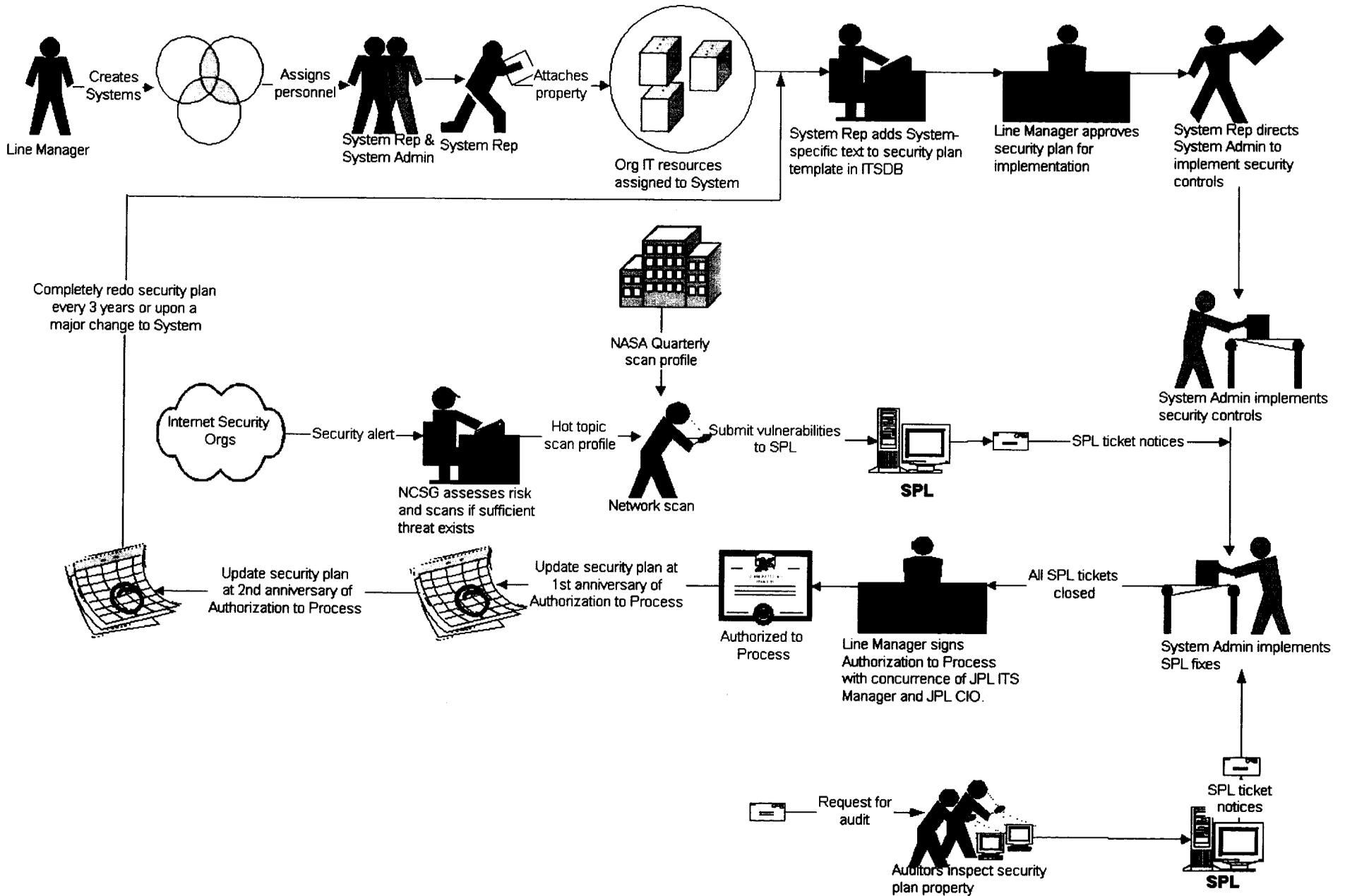
The IT Security Database

- Is the web-based tool to support IT security management
 - IT property inventory
 - IT Systems
 - IT Systems' security plans
- Contains
 - Current data collected from primary sources
 - Rules for conflict resolution
 - Editable templates to facilitate security planning
 - ITSDB supplies format and data available institutionally
 - Users supply content and local data

ITSDB Functional Context



Security Plan Work Flow



Security Problem Log (SPL)

Records security problems found during internal on-site audits and electronic computer security scans

Supports viewing and updating SPL ticket status

Provides weekly reports and metrics to ensure that management is aware of open security vulnerabilities

Addresses risk assessment through a formal (on-line) process for submitting and approving waivers and liens

IT Status Reporting (ITSR)

ITSR is the preferred means of communication when JPL IT Contingency Plan (ITCP) is activated

- Accepts near real-time operational status of all critical Projects and Programs, and their supporting infrastructure
- Displays high-level status, yet permits drill-down for project-specific detail

Promotes coordination among participants

Supports CIO in ensuring operational continuity for critical Projects and Programs

- Comprehensive time-stamped view of all status, good and bad
- Information supports prioritization and allocation of emergency resources, if needed
- Permits IT Emergency Operations Center to be virtual or physical
- Prepares reports for NASA HQ and other centers (if NASA defines format)