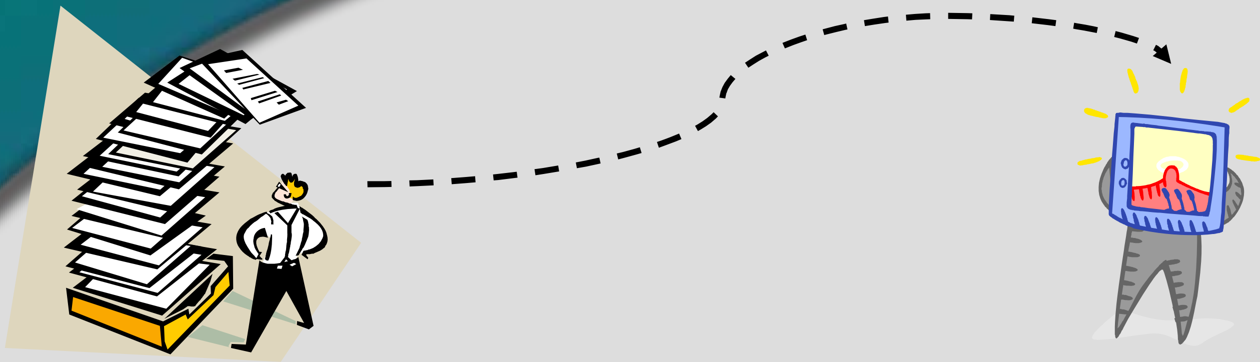


A Tool for Determining Sensitive Computers

Lori Ross O’Neil
Rick Riensche
Pacific Northwest National Laboratory
lro@pnl.gov 509-375-6702

Battelle

Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

Risk Assessment and Sensitivity Determination (RASD) System

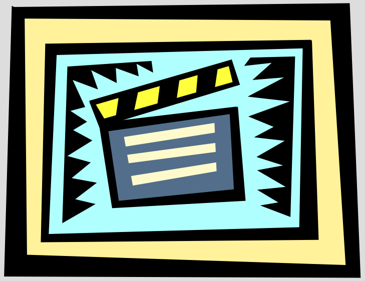
- **R**isk **A**ssessment **S**ensitivity **D**etermination is the process to determine the sensitivity level of computers at PNNL.
- A web-based tool that walks users through sensitivity levels and security plans.
- Knows which systems are sensitive, who owns them, and where they are located.
- Confusing DOE requirements made simple for staff.

Complexity is the deadly enemy of cyber security.

About the RASD Tool

- Uses Entrust digital signatures for approvals.
- The electronic record is the official one. Paper forms are not accepted.
- RASDs are good for 2 years.
- System notifies users to do RASD when
  - new system is received
  - RASD expires
  - system changes ownership.
- Sensitive data types include NNPI, UCNI, FGI, OUO, Intellectual Property, etc.

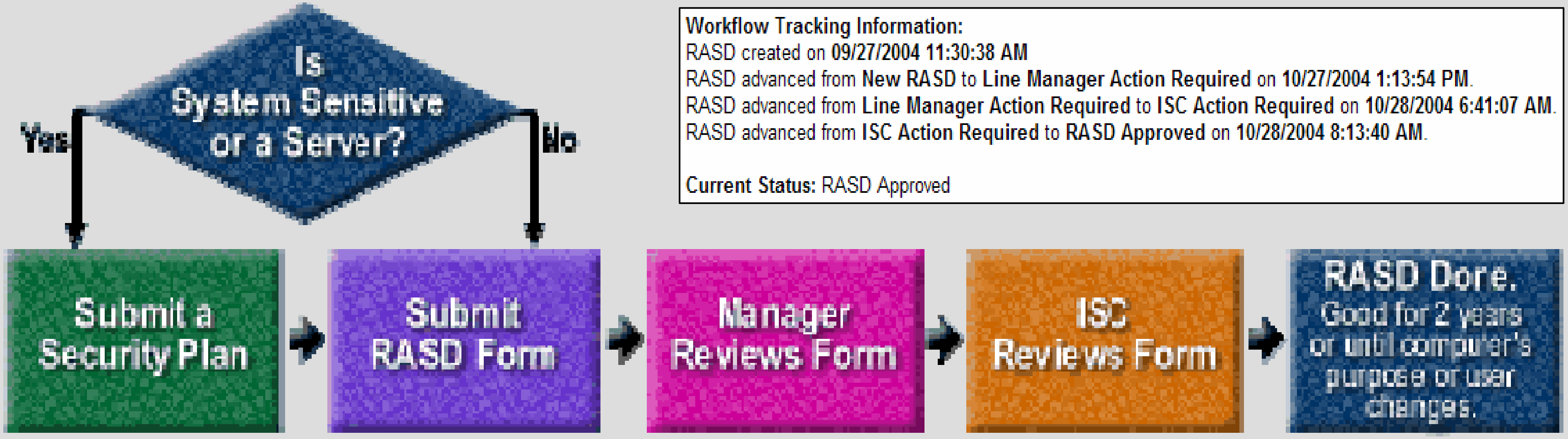
RASD Features



- The application tells the user what systems they have by querying the PNNL Property system.
- Reminds system's owner to submit a RASD. Emails escalate to ISC, line manager, and then to cyber security.
- Reports generated via web tool and metrics are generated nightly.
- Audit trail of process is on every RASD.
- Notifies Property Reps when computers change ownership.

Approval Process

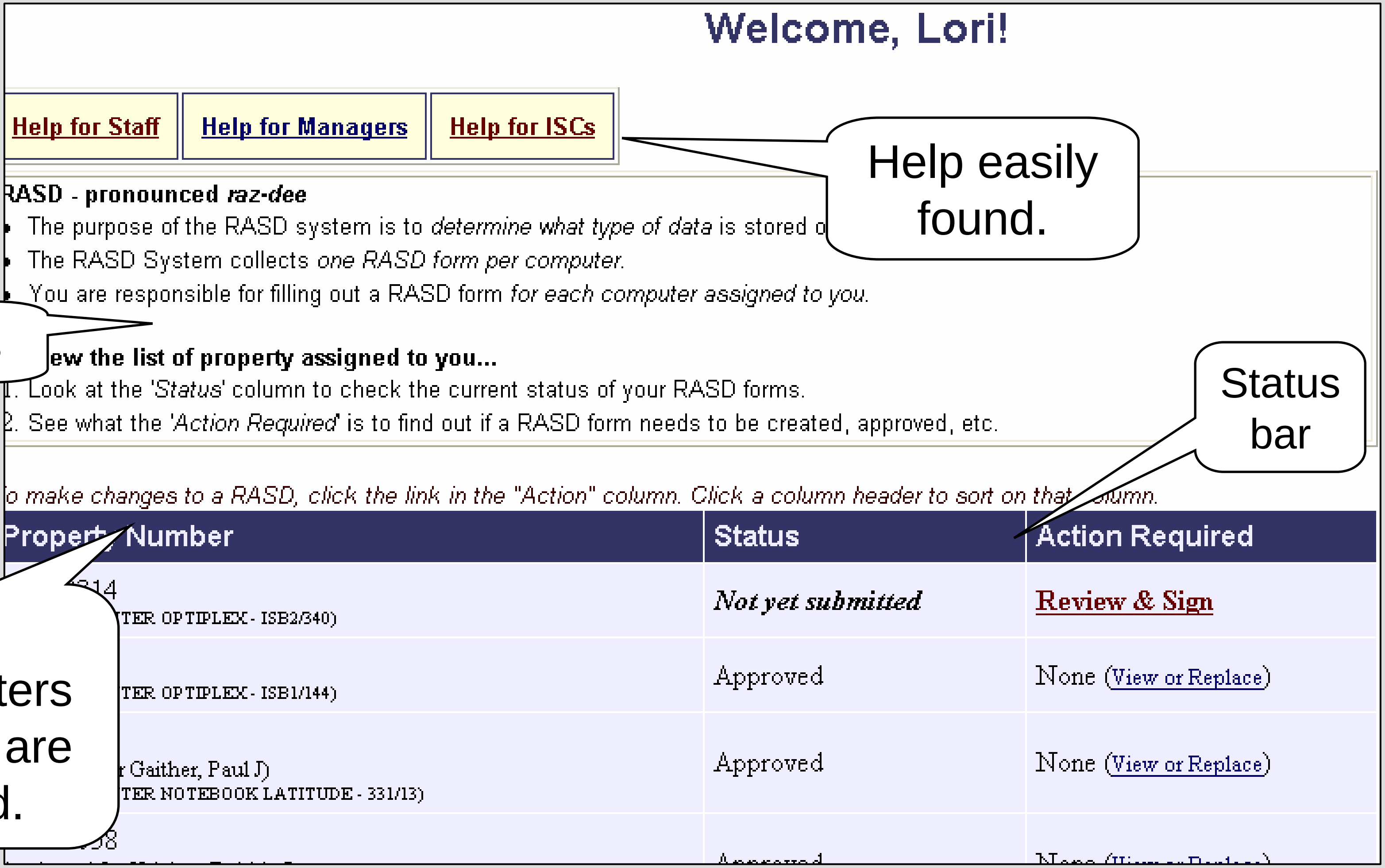
- User completes RASD form and digitally signs it.
- Host's manager reviews form and digitally signs it.
- ISC reviews form and digitally signs it.
- Stored in repository as official record.


Is System Sensitive or a Server?
Yes
No
Submit a Security Plan
Submit RASD Form
Manager Reviews Form
ISC Reviews Form
RASD Done.
Good for 2 years or until computer's purpose or user changes.

Workflow Tracking Information:
RASD created on **09/27/2004 11:30:38 AM**
RASD advanced from **New RASD** to **Line Manager Action Required** on **10/27/2004 1:13:54 PM**.
RASD advanced from **Line Manager Action Required** to **ISC Action Required** on **10/28/2004 6:41:07 AM**.
RASD advanced from **ISC Action Required** to **RASD Approved** on **10/28/2004 8:13:40 AM**.

Current Status: RASD Approved

Dashboard View Homepage



Welcome, Lori!

Help for Staff | Help for Managers | Help for ISCs

Help easily found.

RASD - pronounced *raz-dee*

- The purpose of the RASD system is to *determine what type of data* is stored o
- The RASD System collects *one RASD form per computer.*
- You are responsible for filling out a RASD form *for each computer assigned to you.*

Definitions

ew the list of property assigned to you...

1. Look at the '*Status*' column to check the current status of your RASD forms.
2. See what the '*Action Required*' is to find out if a RASD form needs to be created, approved, etc.

Status bar

o make changes to a RASD, click the link in the "Action" column. Click a column header to sort on that olumn.

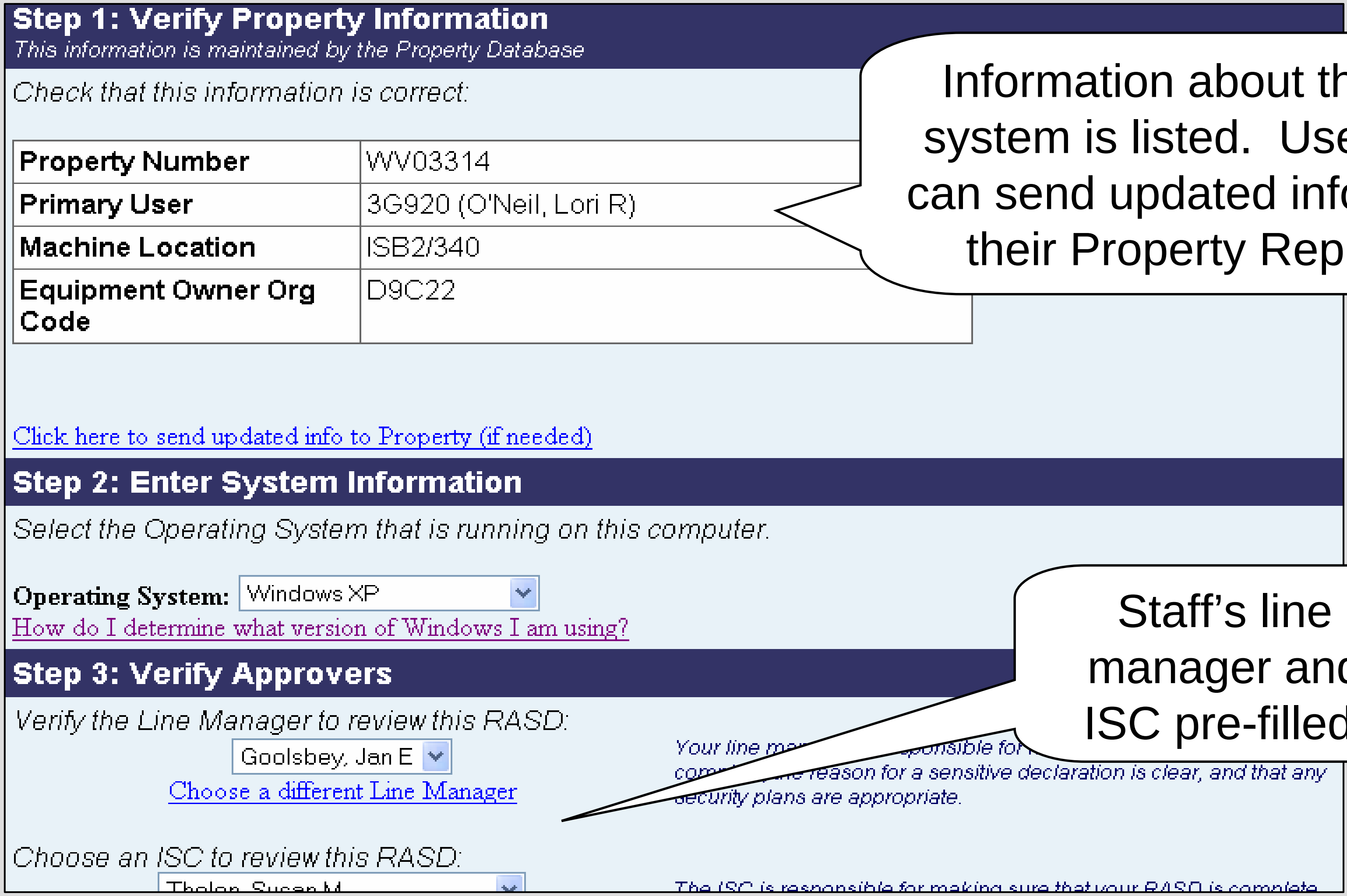
Propert Number	Status	Action Required
314 TER OPTIPLEX - ISB2/340)	***Not yet submitted***	**Review & Sign**
TER OPTIPLEX - ISB1/144)	Approved	None (View or Replace)
r Gaither, Paul J) TER NOTEBOOK LATITUDE - 331/13)	Approved	None (View or Replace)
98	Approved	None (View or Replace)

All computers owned are listed.

Battelle

Pacific Northwest National Laboratory
U.S. Department of Energy

User Is Known



Step 1: Verify Property Information

This information is maintained by the Property Database

Check that this information is correct:

Property Number	WV03314
Primary User	3G920 (O'Neil, Lori R)
Machine Location	ISB2/340
Equipment Owner Org Code	D9C22

Click here to send updated info to Property (if needed)

Step 2: Enter System Information

Select the Operating System that is running on this computer.

Operating System: Windows XP

How do I determine what version of Windows I am using?

Step 3: Verify Approvers

Verify the Line Manager to review this RASD:

Goolsbey, Jan E

Choose a different Line Manager

Your line ma… …ponsible for … com… reason for a sensitive declaration is clear, and that any security plans are appropriate.

Choose an ISC to review this RASD:

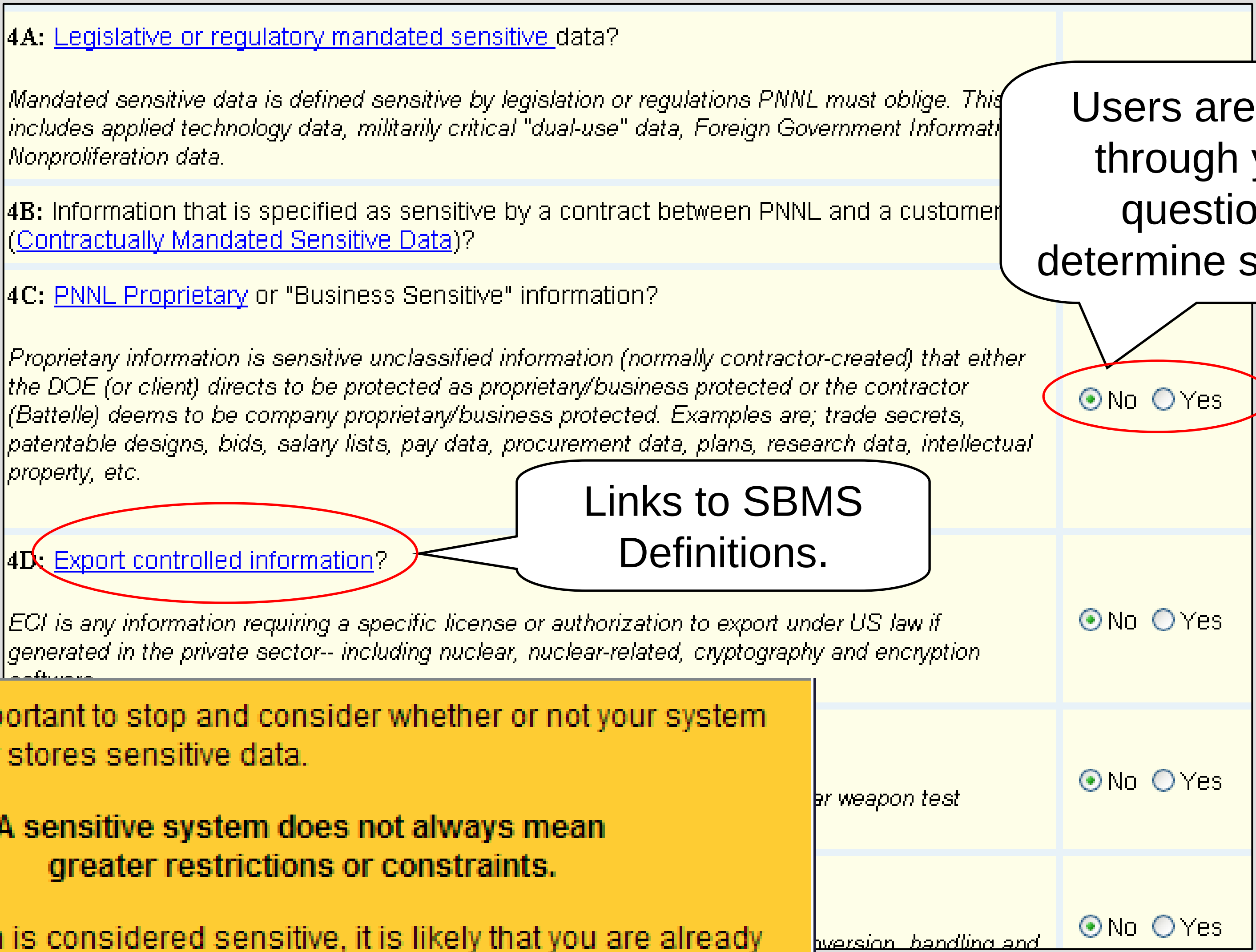
Thelen, Susan M

The ISC is responsible for making sure that your RASD is complete

Information about the system is listed. Users can send updated info to their Property Rep.

Staff's line manager and ISC pre-filled.

Easy to Determine Sensitivity



4A: Legislative or regulatory mandated sensitive data?

Mandated sensitive data is defined sensitive by legislation or regulations PNNL must oblige. This includes applied technology data, militarily critical "dual-use" data, Foreign Government Informati Nonproliferation data.

4B: Information that is specified as sensitive by a contract between PNNL and a customer (Contractually Mandated Sensitive Data)?

4C: PNNL Proprietary or "Business Sensitive" information?

Proprietary information is sensitive unclassified information (normally contractor-created) that either the DOE (or client) directs to be protected as proprietary/business protected or the contractor (Battelle) deems to be company proprietary/business protected. Examples are; trade secrets, patentable designs, bids, salary lists, pay data, procurement data, plans, research data, intellectual property, etc.

● No ○ Yes

4D: Export controlled information?

ECI is any information requiring a specific license or authorization to export under US law if generated in the private sector-- including nuclear, nuclear-related, cryptography and encryption software

● No ○ Yes

r weapon test

● No ○ Yes

version, handling and

● No ○ Yes

Users are walked through yes/no questions to determine sensitivity.

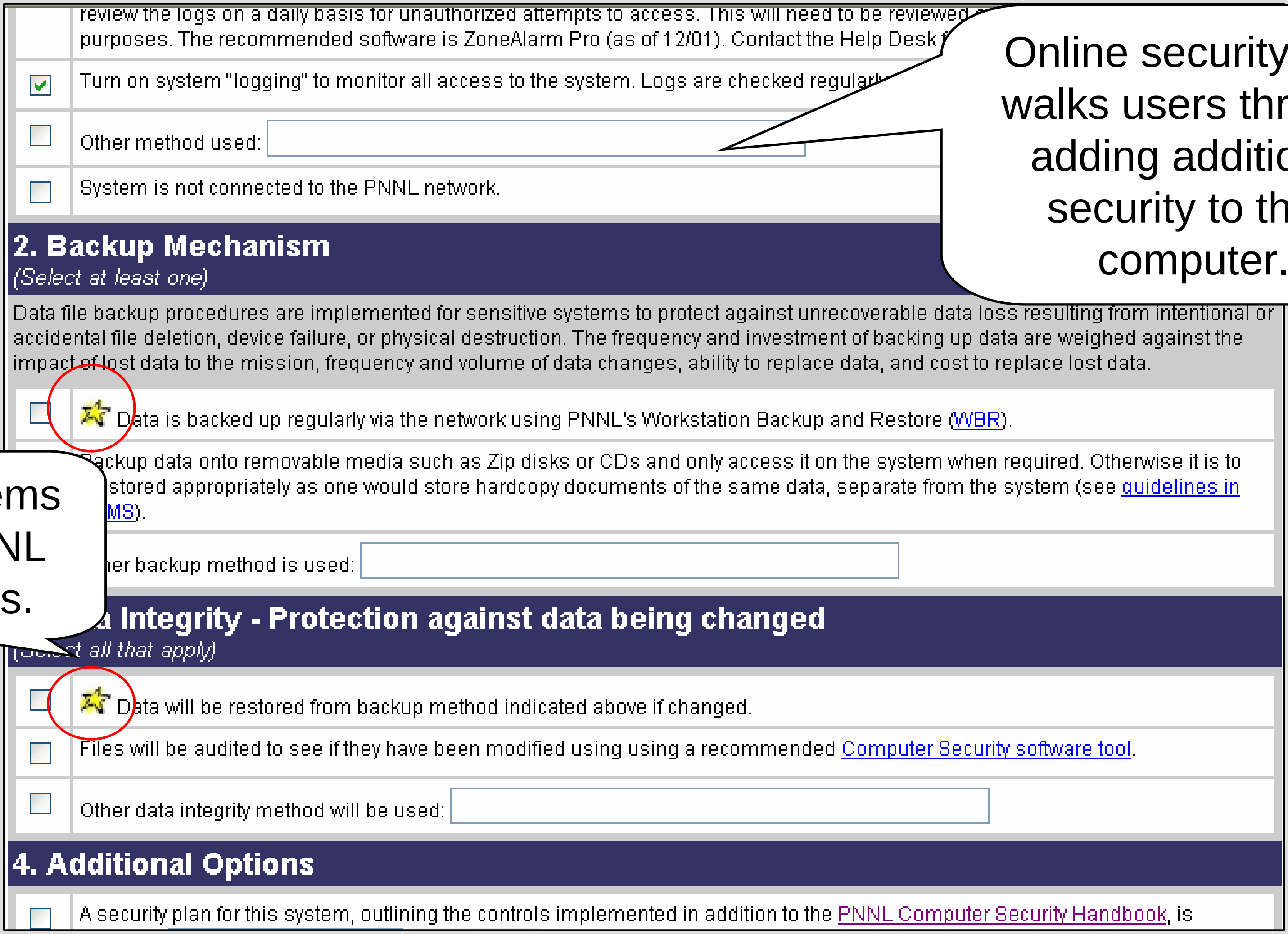
Links to SBMS Definitions.

Note: It is important to stop and consider whether or not your system processes or stores sensitive data.

A sensitive system does not always mean greater restrictions or constraints.

If your system is considered sensitive, it is likely that you are already taking appropriate precautions to protect the system.

Walks User Through Security Plan



review the logs on a daily basis for unauthorized attempts to access. This will need to be reviewed
purposes. The recommended software is ZoneAlarm Pro (as of 12/01). Contact the Help Desk f

☑ Turn on system "logging" to monitor all access to the system. Logs are checked regularl

□ Other method used:

□ System is not connected to the PNNL network.

2. Backup Mechanism
(Select at least one)

Data file backup procedures are implemented for sensitive systems to protect against unrecoverable data loss resulting from intentional or accidental file deletion, device failure, or physical destruction. The frequency and investment of backing up data are weighed against the impact of lost data to the mission, frequency and volume of data changes, ability to replace data, and cost to replace lost data.

□ ☆ Data is backed up regularly via the network using PNNL's Workstation Backup and Restore (WBR).

□ ackup data onto removable media such as Zip disks or CDs and only access it on the system when required. Otherwise it is to stored appropriately as one would store hardcopy documents of the same data, separate from the system (see guidelines in MS).

□ er backup method is used:

a Integrity - Protection against data being changed
t all that apply)

□ ☆ Data will be restored from backup method indicated above if changed.

□ Files will be audited to see if they have been modified using using a recommended Computer Security software tool.

□ Other data integrity method will be used:

4. Additional Options

□ A security plan for this system, outlining the controls implemented in addition to the PNNL Computer Security Handbook, is

Online security plan walks users through adding additional security to their computer.

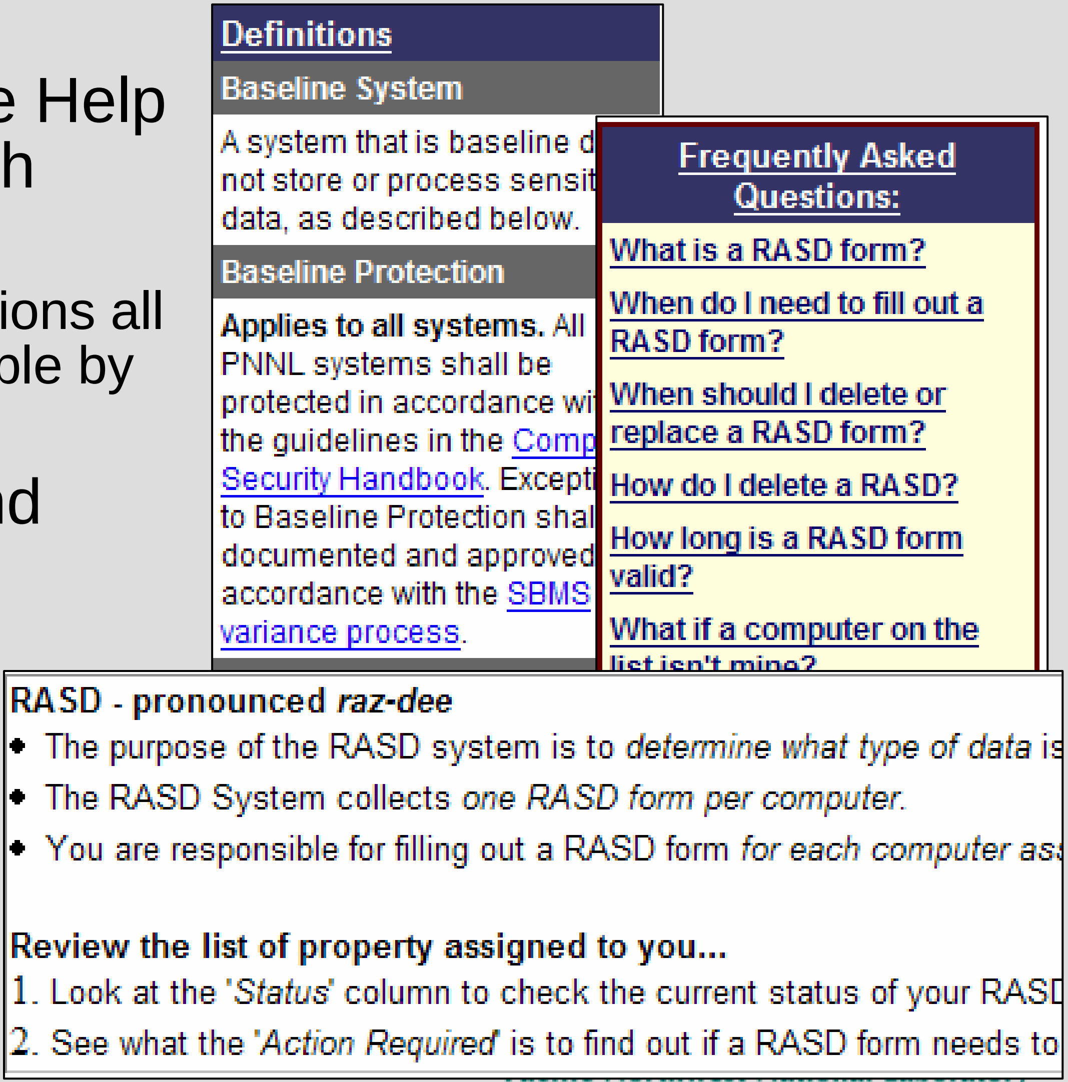
Starred items show PNNL standards.

Update of User Interface

- Application is ~5 years old.
  - Original application grew from “proof-of-concept” prototype with a very rudimentary user interface.
- 3 years ago UI was updated.
  - In 2002 we enlisted the help of PNNL usability experts from the Rich Interaction Environments group.
  - Formal study
    - Observing and recording user reactions to software while performing a scripted set of tasks
    - Producing an end result of a proposed design update

Results of UI Redesign

- Added FAQ and made Help links cleaner and much more prominent.
  - FAQ, Help, and Definitions all database-driven; editable by RASD Administrator.
- Better organization and clarity of questions.
- Drastically improved appearance.



Definitions

Baseline System

A system that is baseline d
not store or process sensit
data, as described below.

Baseline Protection

Applies to all systems. All PNNL systems shall be protected in accordance wi the guidelines in the Comp Security Handbook. Excepti to Baseline Protection shal documented and approved accordance with the SBMS variance process.

Frequently Asked Questions:

What is a RASD form?

When do I need to fill out a RASD form?

When should I delete or replace a RASD form?

How do I delete a RASD?

How long is a RASD form valid?

What if a computer on the list isn't mine?

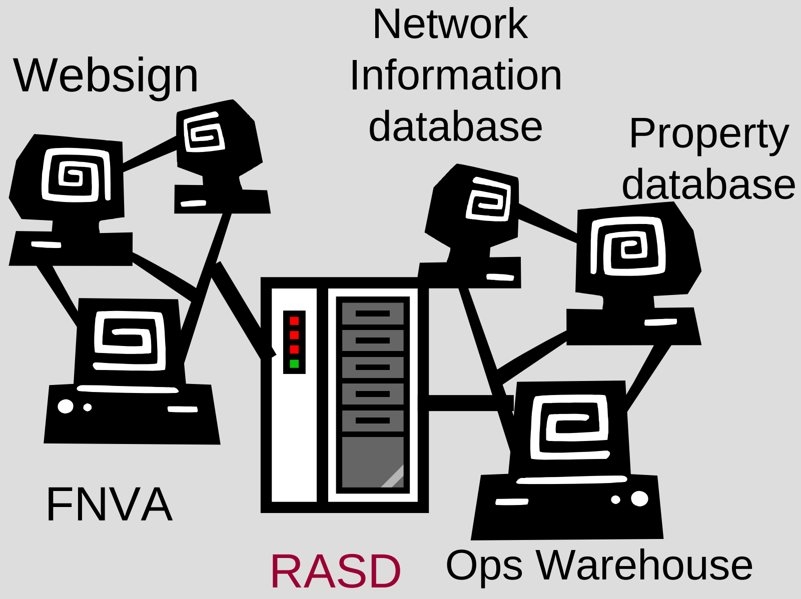
RASD - pronounced *raz-dee*

- The purpose of the RASD system is to *determine what type of data is*
- The RASD System collects *one RASD form per computer.*
- You are responsible for filling out a RASD form *for each computer as*

Review the list of property assigned to you...

1. Look at the '*Status*' column to check the current status of your RASD
2. See what the '*Action Required*' is to find out if a RASD form needs to

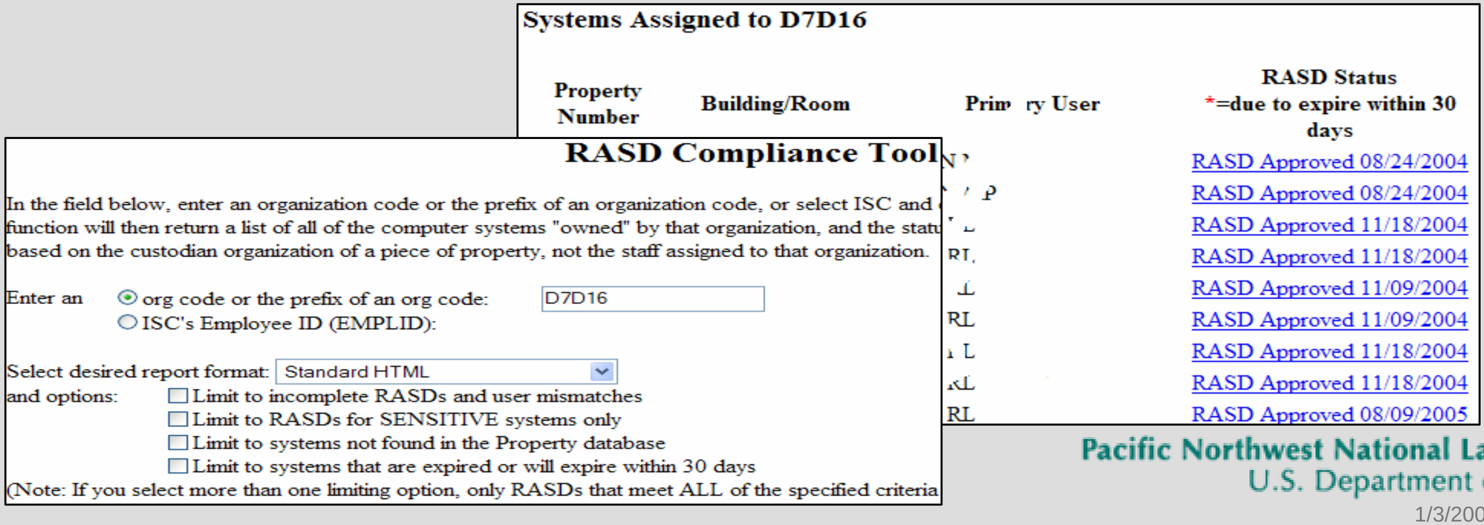
Many Databases Used



- RASD draws extensively from external databases.
  - Property database
  - “Ops Warehouse” Employee information
  - Network database
- RASD also interacts with external systems.
  - Digital Signature System (websign)
  - Foreign National Visit/Assignment (FNVA)

Handy Features of RASD

- Reporting functionality allows ISCs and UCS staff to extract actionable data from RASD.
  - Compliance reporting
    - Available in HTML or Excel formats
    - Summarizes by Org Code or by ISC
    - Higher-level reports for upper-level management
    - Specialized reports (for example, long overdue RASDs)
  - Historical lookup
    - Old RASDs aren't truly "deleted" and can be queried by ISCs.



Systems Assigned to D7D16

Property Number	Building/Room	Prim ry User	RASD Status *=due to expire within 30 days
		N	RASD Approved 08/24/2004
		P	RASD Approved 08/24/2004
		L	RASD Approved 11/18/2004
		RI	RASD Approved 11/18/2004
		L	RASD Approved 11/09/2004
		RL	RASD Approved 11/09/2004
		L	RASD Approved 11/18/2004
		RL	RASD Approved 11/18/2004
		RL	RASD Approved 08/09/2005

RASD Compliance Tool

In the field below, enter an organization code or the prefix of an organization code, or select ISC and
function will then return a list of all of the computer systems "owned" by that organization, and the statu
based on the custodian organization of a piece of property, not the staff assigned to that organization.

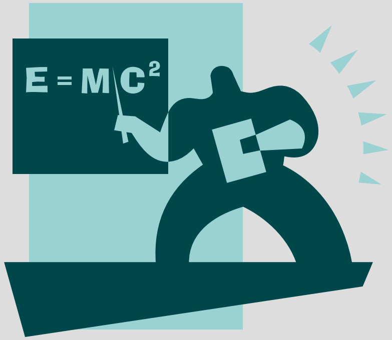
Enter an ● org code or the prefix of an org code: D7D16
○ ISC's Employee ID (EMPLID):

Select desired report format: Standard HTML

and options:
□ Limit to incomplete RASDs and user mismatches
□ Limit to RASDs for SENSITIVE systems only
□ Limit to systems not found in the Property database
□ Limit to systems that are expired or will expire within 30 days

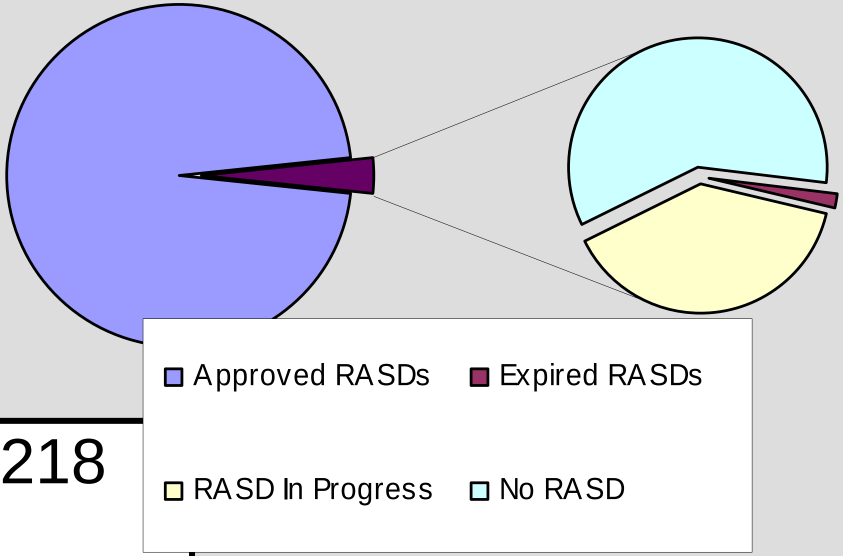
(Note: If you select more than one limiting option, only RASDs that meet ALL of the specified criteria

Lessons Learned



- If at first you don’t succeed, do a user interface study.
- The customer isn’t always right – as a developer, you need to be smart, communicate well, and think ahead to what they’ll want next.
- Understand the customer’s business and help them bring it into the computer age.
- External dependencies affect development – sometimes severely!

RASD Metrics



Total Computer Systems:	16218
Approved RASDs:	15622
Expired RASDs:	12
RASD In Progress:	230
No RASD:	354
% with Approved RASD:	96.3%

Thank you for your interest!

- RASD is available for use to other DOE labs through the PNNL *Government Use Acknowledgement Agreement.*
- Built in IBM Lotus Notes.
- Developed by Rick Riensche.
- Contact Lori Ross O'Neil, 509-375-6702, lro@pnl.gov

Risk Assessment and Sensitivity Determination (RASD) System