Evaluating Computer Vulnerabilities in Near Real Time

Lori Ross O'Neil

Phil Capiral

Pacific Northwest National Laboratory

lro@pnl.gov 509-375-6702

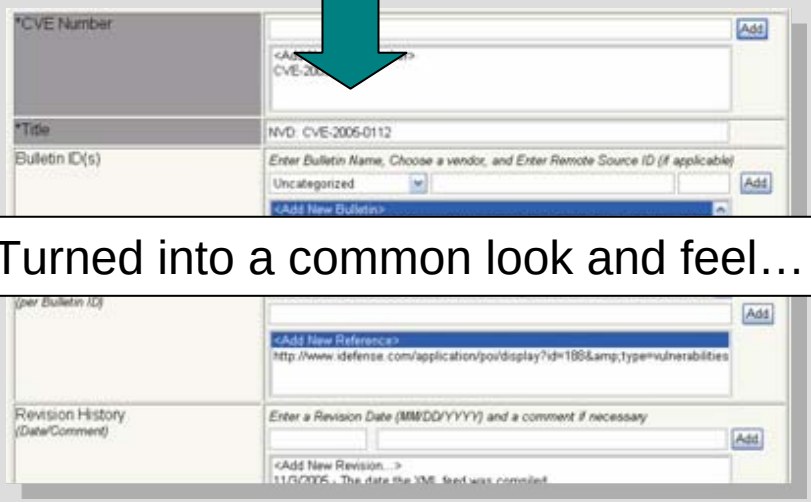
Many sources…

redhat.

Sponsored by DHS National Cyber Security Division/US-CERT
National Vulnerability Database
a comprehensive cyber vulnerability resource
NIST National Institute of Standards and Technology

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Microsoft



Turned into a common look and feel…

Reviewed	Un	eview	Completed	Percentage
199	30		93	46.73%

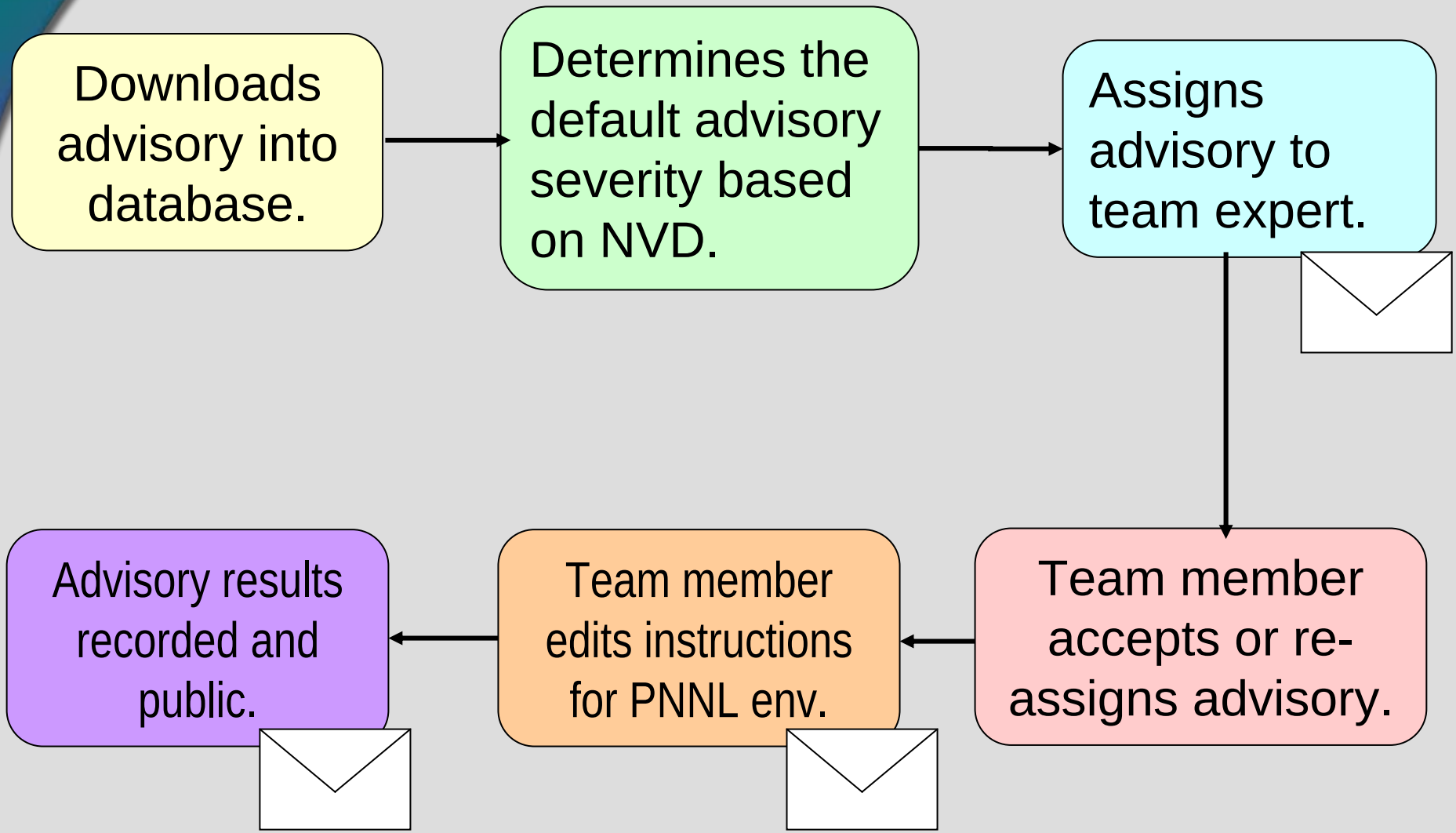
vote	Count
Immediate	2
Required	90
Recommended	100
Acceptable Risk	6
Reject	1
Network Infrastructure	14
PDAs	1
Software Application	9
UNIX/Linux	109

Produces a cohesive solution.

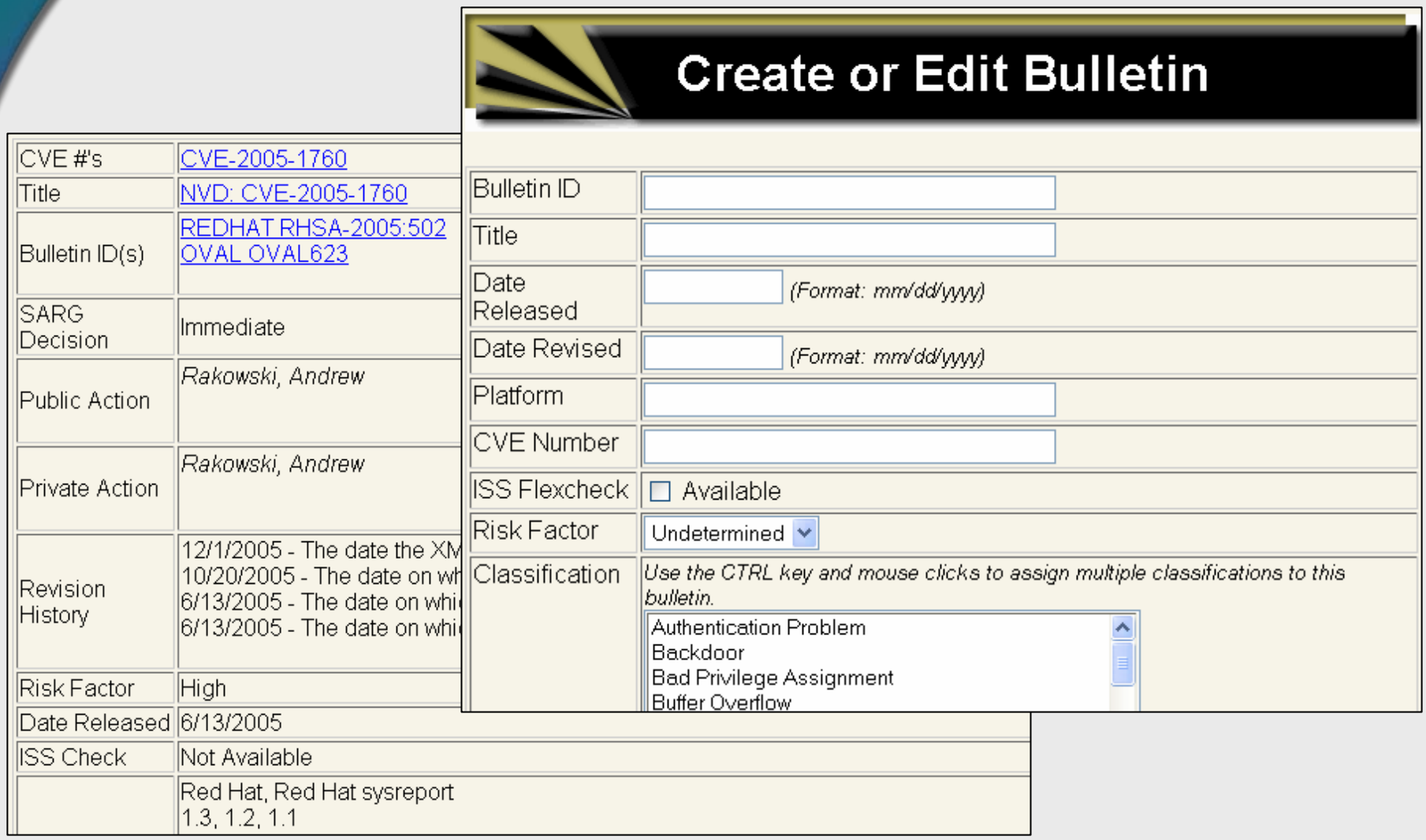
What Is Security Advisory Review Tool?

- SART was developed to automate and speed up the process of reviewing security vulnerabilities, assigning responsibility, and taking action.
- Web-based tool allows team members to act on vulnerabilities with respect to PNNL's computing environment.
- Turnaround for vulnerabilities is less than a week from voting to action (previously months).
- Data entered manually or via XML feed from NIST.
- Tracks by CVE (Common Vulnerabilities and Exposures).

SART Process Flow



1. Manual or Automatic Input

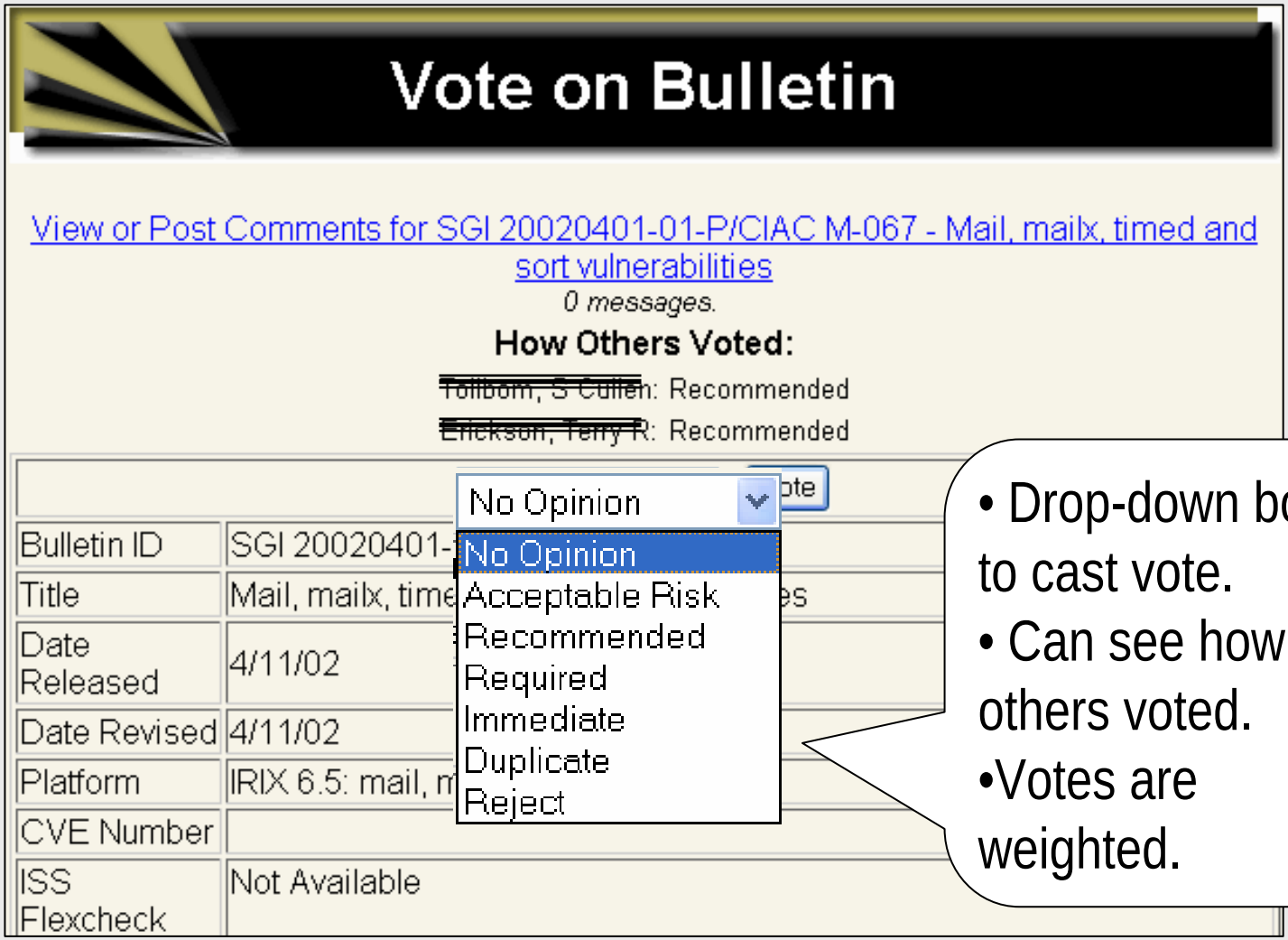


CVE #'s	CVE-2005-1760
Title	NVD: CVE-2005-1760
Bulletin ID(s)	REDHAT RHSA-2005:502 OVAL OVAL623
SARG Decision	Immediate
Public Action	*Rakowski, Andrew*
Private Action	*Rakowski, Andrew*
Revision History	12/1/2005 - The date the XM 10/20/2005 - The date on wh 6/13/2005 - The date on whi 6/13/2005 - The date on whi
Risk Factor	High
Date Released	6/13/2005
ISS Check	Not Available
	Red Hat, Red Hat sysreport 1.3, 1.2, 1.1

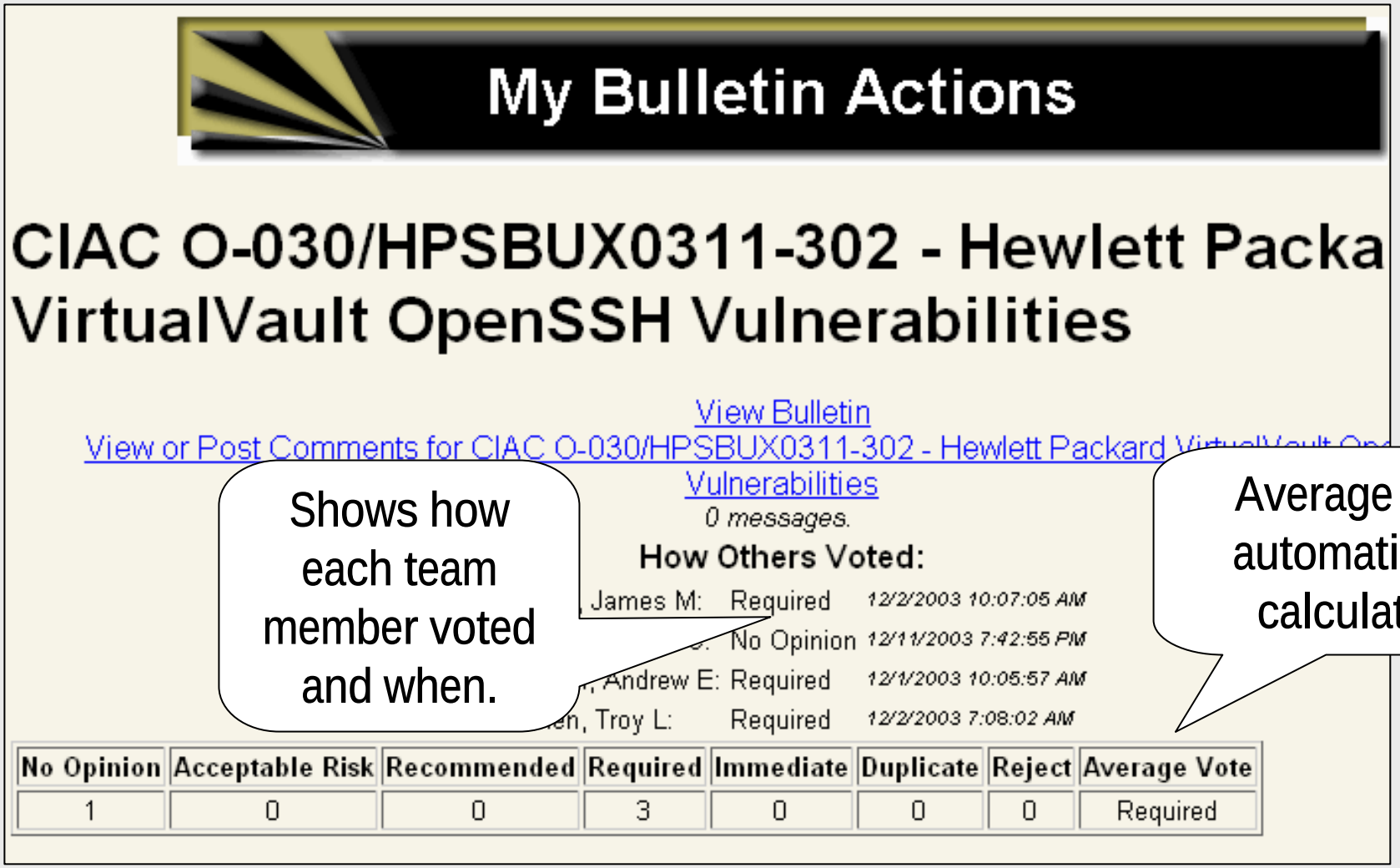
Create or Edit Bulletin

Bulletin ID	
Title	
Date Released	*(Format: mm/dd/yyyy)*
Date Revised	*(Format: mm/dd/yyyy)*
Platform	
CVE Number	
ISS Flexcheck	☐ Available
Risk Factor	Undetermined
Classification	*Use the CTRL key and mouse clicks to assign multiple classifications to this bulletin.* Authentication Problem Backdoor Bad Privilege Assignment Buffer Overflow

2. Team Members Vote



3. SART Assigns Responsibility



4. Assigned Team Member Closes

Bulletin ID	ISS Advisory
Title	Wired-side SNMP key exposure in 802.11b Access Points
Date Released	6/20/01
Date Revised	6/20/01
Team Decision	Recommended
Completion Comments	
Public Action	This vulnerability does not affect PNNL's wireless LAN, but as you may have customers that could be affected by this, please make them aware of
Private Action	
	Submit Action
Platform	3Com and Symbol wired access devices
CVE Number	CAN-2001-0352

Public Action

Private Action

Public action can be viewed by Lab staff.

Private action only viewed by SART team.

5. Admin Maintains Lists via SART

Edit Mailing Lists

Mailing List ID	Mailing List Name	Mailing List Description	
9	Database	Database related vulnerabilities and patches	Edit
7	Macintosh	Macintosh Vulnerabilities and Patches	Edit
8	Network Infrastructure	Hardware Vulnerabilities and Patches	Edit
11	PDAs	Personal Digital Assistant Vulnerabilities and Patches	Edit
13	Software Application	Various software applications	Edit
3	UNIX/Linux	UNIX or Linux OS Vulnerabilities and Patches	Edit
2	Web services	Web servers and services vulnerabilities and patches	Edit
4	Windows 2000	Windows 2000 OS Vulnerabilities and Patches	Edit
6	Windows 95/98	Windows 95/98 Vulnerablilities and Patches	Edit
12	Windows Me	Windows Me Vulnerabilities and Patches	Edit

Unused Software Vendors

1-Script
10-4 APS
1Two
427BB
4D
88Script
AaronOutpost
AbcZone.it
AbiSource
Abuse-SDL
Accelerated E Solutions
Access user Class

Assignments

Keyword	Sarg Member
Apple	Adam
Computer Associates	Alexa
IBM	Alexa
VMWare	Alexa

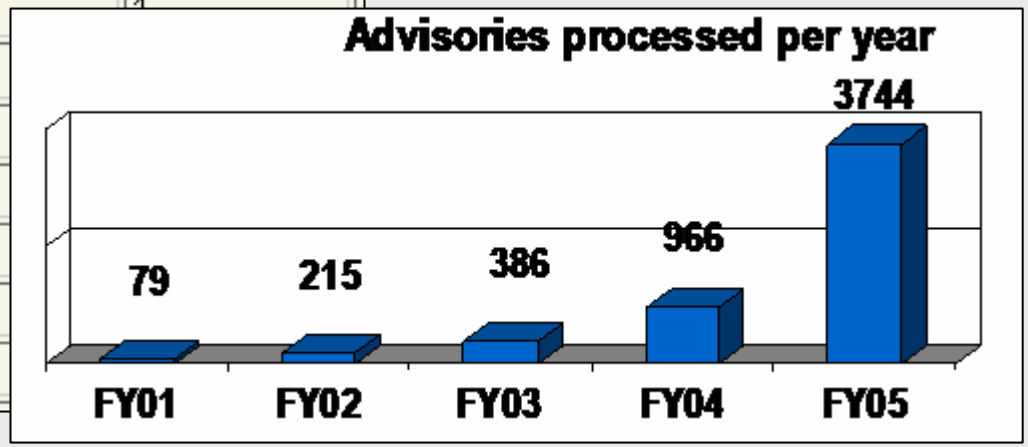
- Mailing Lists
- Team Members
- Vulnerability Classifications
- Vendors

6. SART Generates Metrics

Reviewed	Under Review	Completed	Percentage
199	30	93	46.73%

Final Vote	Count
Immediate	2
Required	90
Recommended	100
Acceptable Risk	6
Reject	

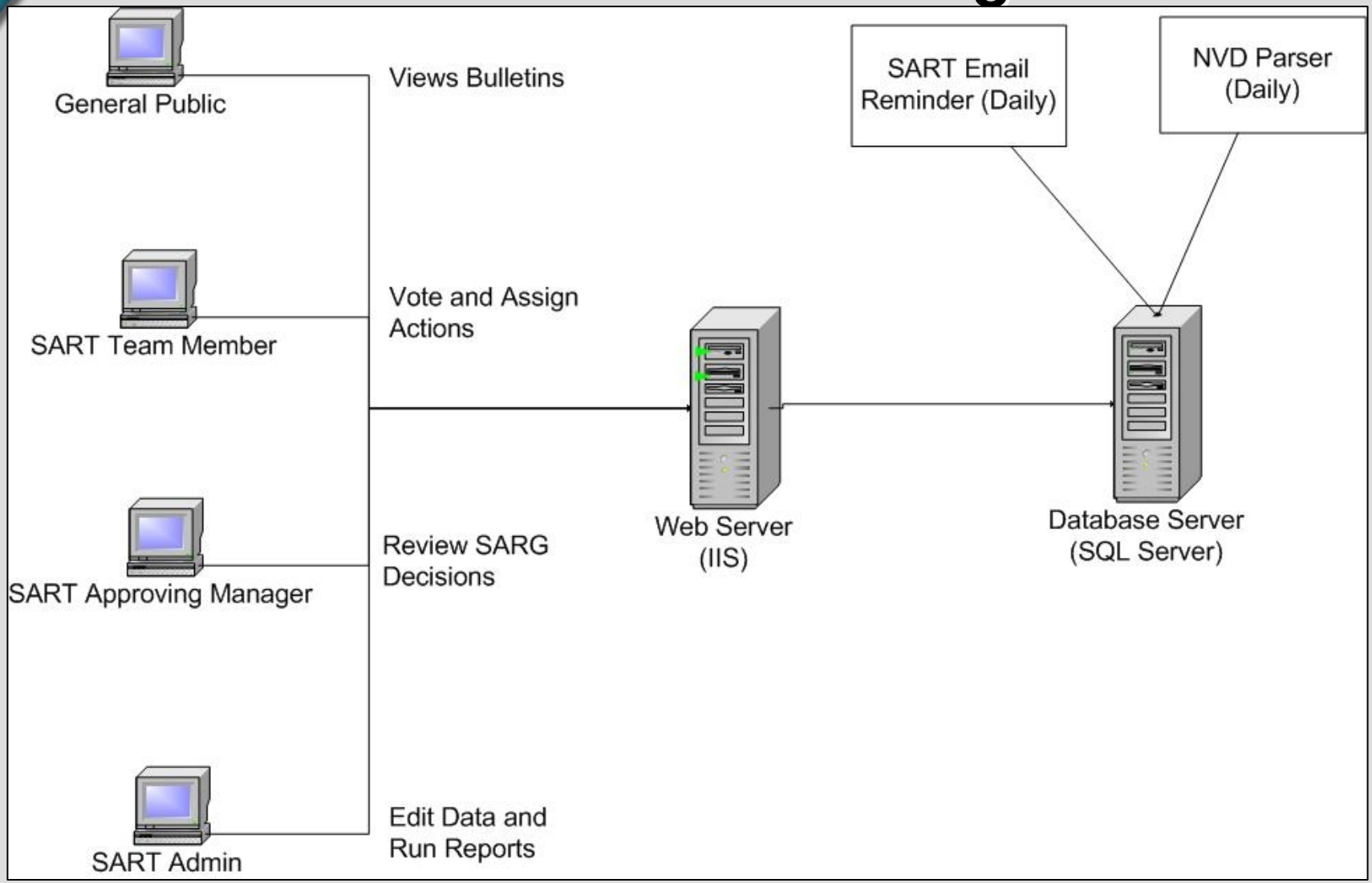
Platform
Database
Macintosh
Network Infrastructure
PDAs
Software Application



SART Development Facts

- Database platform is SQL Server
- Built on ASP.NET
- Runs IIS Server version 5.0 or later
- Uses SMTPMail Mail Engine
- Customized interface based on user access level (DB Admin, SART Admin, Team Member)
- Developed by Phil Capiral and Brian Vladimiroff

SART Process Design



SART Development Challenges

- There are too many vulnerabilities to act on
  - Hard to keep up with data entry
  - Batch voting
- There are too many vulnerabilities to assign
  - Default assignments
  - NIST soon to implement a standard scoring system (CVSS)
- It is hard to associate vulnerabilities with other systems
  - Use CVE as unique identifier

Thank you for your interest!

- SART is available for other DOE labs to use through the PNNL *Government Use Acknowledgement Agreement.*
- Has been shared with
  - Lawrence Livermore National Lab
  - Honeywell Kansas City
  - Sandia National Lab
  - Savannah River Site
  - Oakridge National Lab
- Contact Lori Ross O'Neil, 509-375-6702, lro@pnl.gov