The following power point presentation is a draft based on previous Committee meetings. The presentation just lists basic information at this time. Pictures, animations, examples, etc., will be added after the Committee reviews the slides for content. This may be the last time the Committee can review the message content before the CLJ court administrators' training in May.

JIS Security and Data Confidentiality for District / Municipal Court Administrators

Topics

- Access
- Data Confidentiality
- RACFID Set-Up and Monitoring
- RACFID Use

Access to Court Records

- Washington State Constitution, Article 1 Section 10
  - Justice in all cases shall be administered openly, and without unnecessary delay
- GR 31 – Access to Court Records
- Transparency
- Accessible

Confidential Information

- Access is restricted by:
  - Statutory and/or common law
  - Court Rules
  - Court Order
- Court staff has access to confidential information
- Duty to ensure that the confidential information is protected – <u>once the information is labeled confidential</u>

CONFIDENTIAL INFORMATION

How do I know if information is confidential?

- What does the file or document say
- Is there a statute
- Refer to GR 31, GR 22, GR 15
- Is there a court order
- Consult with your Prosecuting Attorney
- Call me at 360-705-5315

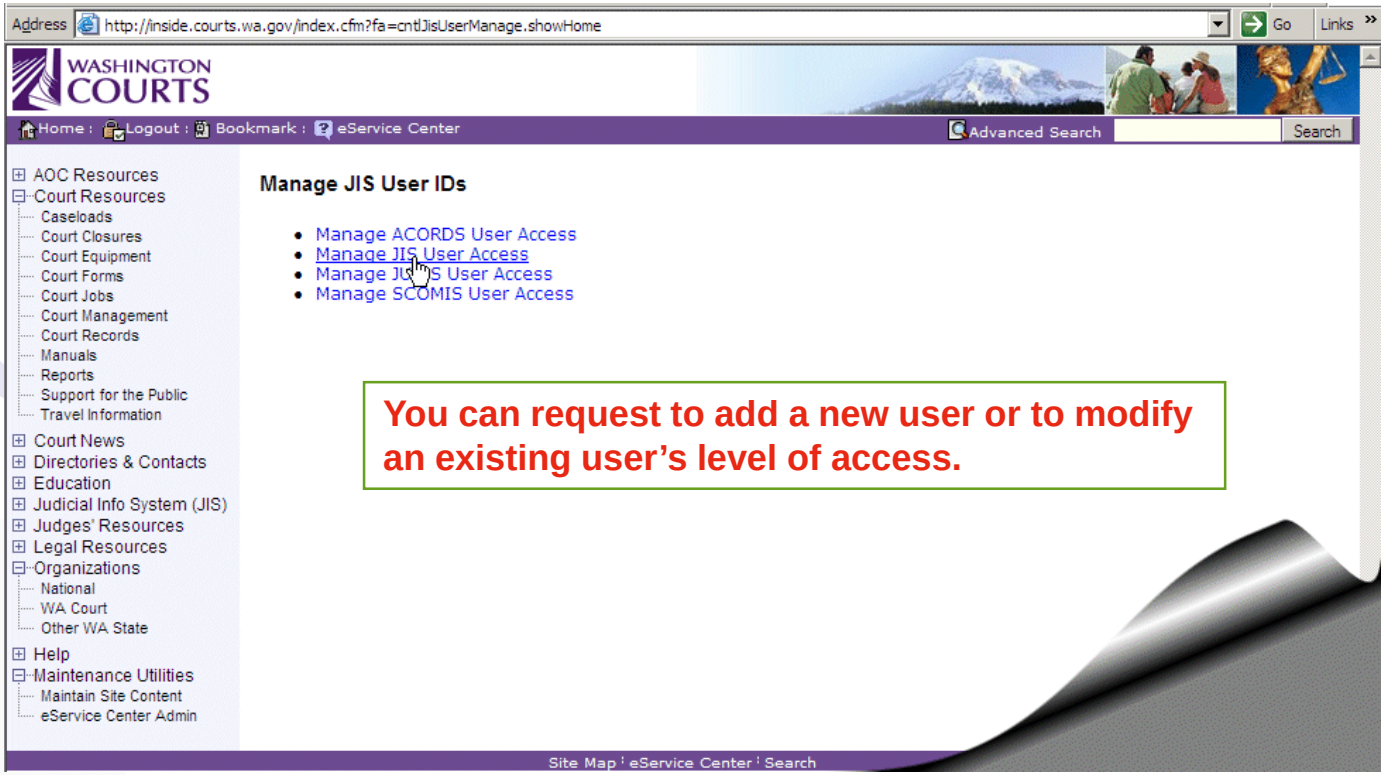
Data Confidentiality: Examples

- Case index screens are public but a court user's view shows more information
- Case history screens are not public
- Reports may contain data that is not public (e.g., Docket Report and the Court Calendar)
- Personal identifiers and screens are not public
- DOL's Abstract of Driving Record is not public

CONFIDENTIALITY AGREEMENTS

- Access only for job-related purposes
- Only divulge to authorized people
- Only divulge to others if authorized
- Report breaches or potential breaches of release of confidential information to you
- Staff should consult supervisors if questions

Managing User IDs



(Manage JIS User Access)

Setting Up and Maintaining JIS Security for Court Officials and Staff

- (*optional*) Search for officials **(OOD)**
- Create Official Person record for AM, AC, CH, CL, and JG officials **(OFOA)**
- Create security authorizations for AC, CH, CL, and JG officials **(ATHA)**
- Modify security authorizations **(ATHX**)
- Maintain security profiles & passwords (**ATH**)
- Delete security authorizations (**ATHD**)

When staff needs different security:

Manage User ID: Modify Existing User

- Role Changes--site coordinator , authorized caller, or printing automated checks
- Note: For name changes or role changes do the "Leaves Court" tasks then do the "New User" tasks.

When staff needs different security:

JIS: Change security settings

- ATH to change receipt printer (example: desk location changed, closer to a different receipt printer)
- ATHX to change screen or utility security (example: needs access to
additional screens due to new duties)

When Staff Leaves the Court:

1. date the OFO

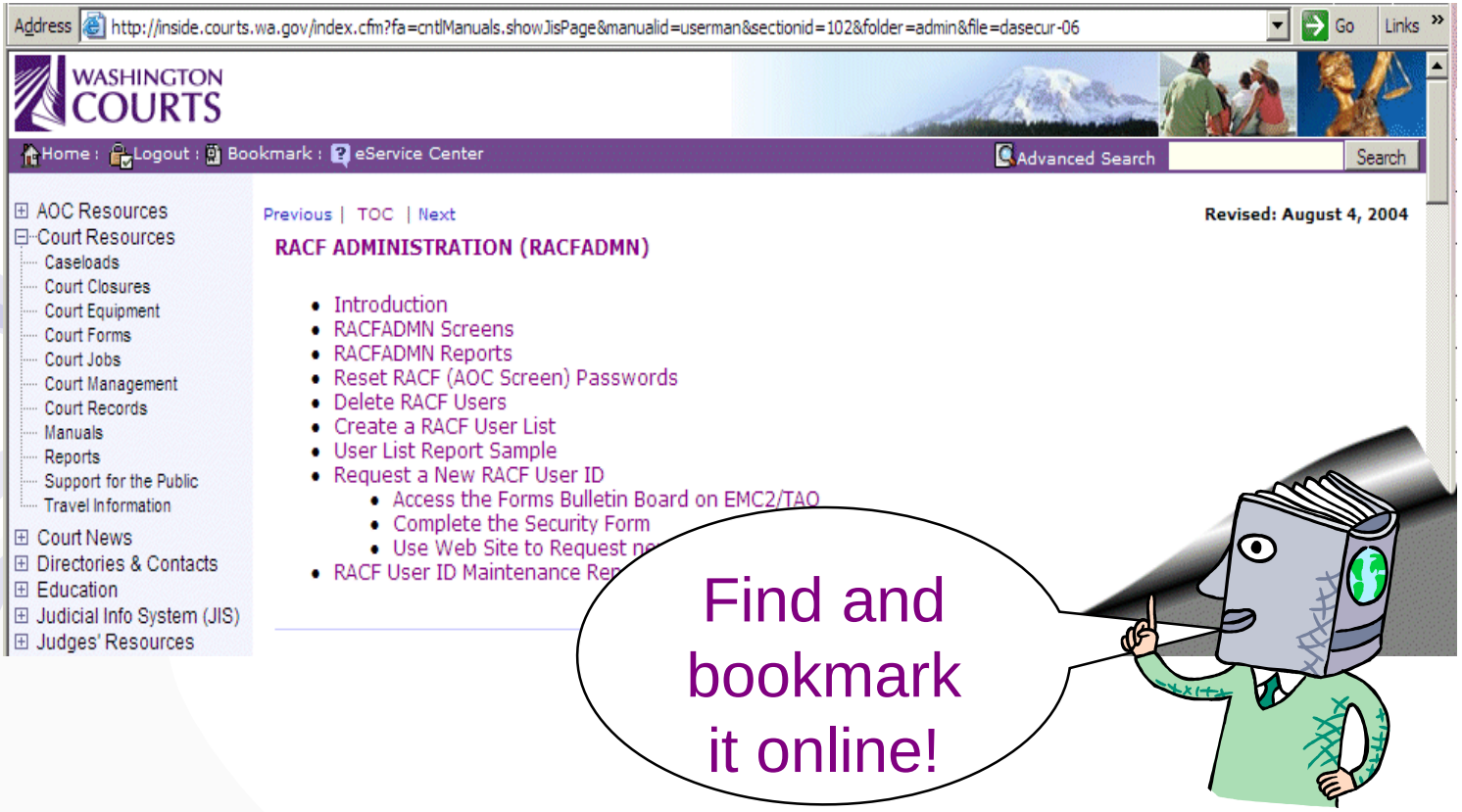
2. ATH to delete the

3. ATHD to delete the JIS

4. RACFAD MN to delete the

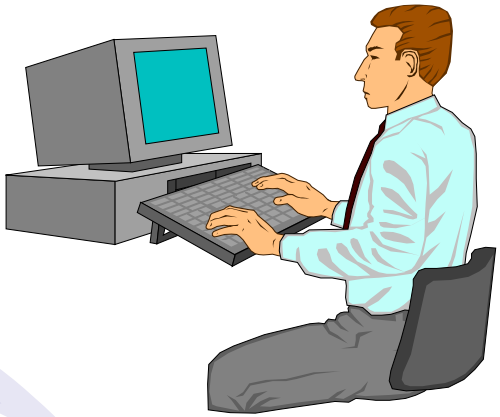
A ***Deleted User Report*** is generated and initiates an eService Center incident.

JIS online manual documentation on the RACFADMN utility



Self-Maintenance of Sign-on (UserID/RACF ID) Password

- Encourage staff to self-register online for User ID password reset service
- “Blockade” is AOC’s self service security system
- After registering, you can reset the password for your User ID, even if you’ve forgotten the old password



Review Your Court's

User Lists:

- ✓ Active User List
- ✓ Site User List

RACFID Misuse

- Setting up a user who is not a court employee
- Providing access that does not match the user’s position
- Looking up information for personal reasons
- Sharing sensitive and confidential data